Política de Certificación de Certificados de Firma electrónica

ANFAC Autoridad de Certificación Ecuador C.A
Av. 12 de Octubre N24-739 y Av. Colon - Ed. Torre Boreal
170143 - Quito (Ecuador)
Teléfono: +593 02 3826877
Web: www.anf.ec

Nivel de Seguridad

Público

Aviso Importante

Dirección: Av. 12 de Octubre N24-739 y Av. Colon - Ed. Torre Boreal 170143 - Quito (Ecuador)

Teléfono: +593 02 3826877 - Web: www.anf.ec

Índice

1 Introducción 6
1.1. Descripción de los certificados 7
1.1.1. Certificado Electrónico/digital de Persona Física 8
1.1.2. Certificado Electrónico/digital de Persona Jurídica, Representante legal o Empleado con relación de dependencia 8
1.1.3. Certificados de Empleado Público 9
1.2. Nombre del documento e identificación 10
1.3. Partes de la PKI 10
1.4. Ámbito de aplicación 10
1.4.1. Usos permitidos 10
1.4.2. Límites de uso de los certificados 11
1.4.3. Usos prohibidos 11
1.5. Datos de contacto de la Entidad de Certificación 11
1.6. Definiciones y Acrónimos 11

2. Repositorios y publicación de la información 12
2.1. Repositorios 12
2.2. Publicación de la información 12
2.3. Frecuencia de actualizaciones 12
2.4. Controles de acceso a los repositorios 12

3. Identificación y Autenticación 13
3.1. Registro de nombres 13
3.1.1. Tipos de nombres 13
3.1.2. Guía de cumplimentación de campos específicos 13
3.1.3. Necesidad de que los nombres sean significativos 14
3.1.4. Seudónimos o anónimos 14
3.1.5. Reglas utilizadas para interpretar varios formatos de nombres 14
3.1.6. Unicidad de los nombres 14
3.1.7. Resolución de conflictos relativos a nombres y marcas 14
3.2. Validación inicial de la identidad 14
3.2.1. Prueba de posesión de clave privada 14
3.2.2. Autenticación de la identidad del suscriptor 15

3.3. Renovación de la clave 15
3.4. Solicitud de revocación 15

4. Requisitos Operacionales 16
4.1. Interoperabilidad y Seguridad. 16
4.1.1. Operación y gestión de la Infraestructura de Clave Pública 16
4.1.2. Interoperabilidad 16
4.2. Solicitud del certificado 16
4.3. Procedimiento de tramitación 16
4.3.1. Autenticación de identidad 16
4.3.2. Aprobación o rechazo de las solicitudes de certificados 19
4.3.3. Tiempo para procesar la emisión de certificados 20
4.4. Emisión del certificado 21
4.4.1. Acciones de la Entidad de Certificación durante el proceso de emisión 21
4.4.2. Notificación al suscriptor 21
4.5. Aceptación del certificado 21
4.5.1. Aceptación 21
4.5.2. Devolución 21
4.5.3. Seguimiento 22
4.5.4. Publicación del certificado 22
4.5.5. Notificación de la emisión del certificado a terceros 22
4.6. Denegación 22
4.7. Renovación de certificados 22
4.7.1. Certificados vigentes 22
4.7.2. Personas autorizadas para solicitar la renovación 22
4.7.3. Identificación y autenticación de las solicitudes de renovación rutinarias 23
4.7.4. Aprobación o rechazo de las solicitudes de renovación 23
4.7.5. Notificación de la renovación del certificado 23
4.7.6. Aceptación de la renovación del certificado 23
4.7.7. Publicación del certificado renovado 23
4.7.8. Notificación a otras entidades 24
4.7.9. Identificación y autenticación de las solicitudes de renovación de clave después de una revocación -Clave no comprometida- 24
4.8. Modificación del certificado 24
4.9. Revocación y suspensión de certificados 24
4.9.1. Causas de revocación 24
4.9.2. Identificación y autenticación de solicitudes de revocación 24
4.9.3. Procedimiento para la solicitud de revocación 25
4.9.4. Periodo de gracia de la solicitud de revocación 26
4.9.5. Plazo máximo de procesamiento de la solicitud de revocación 26

4.9.6. Requisitos de comprobación de listas CRL 26
4.9.7. Frecuencia de emisión de CRL 26
4.9.8. Disponibilidad de comprobación on-line de la revocación 26
4.9.9. Requisitos de la comprobación on-line de la revocación 26
4.9.10. Suspensión del certificado 26
4.9.11. Identificación y autenticación de solicitudes de suspensión 27
4.10. Depósito y recuperación de claves 27

5. Controles de seguridad física, instalaciones, gestión y operacionales 28
5.1. Controles de seguridad física 28
5.2. Controles de procedimiento 28
5.3. Controles de personal 28

6. Controles de seguridad técnica 29

7. Perfiles de certificados, listas CRL y OCSP 30
7.1. Perfiles de certificados 31
7.2. Perfil de CRL 31
7.3. Perfil de OCSP 32

8. Auditoría de conformidad 33

9. Disposiciones generales 34

1 Introducción

ANFAC AUTORIDAD DE CERTIFICACION ECUADOR C.A., en adelante, **ANF AC**, es una entidad jurídica, legalmente constituida, inscrita en el Registro Mercantil del Cantón de Quito, con el número de inscripción 3760 y RUC 1792601215001.

Acreditada por ARCOTEL como Entidad de Certificación de Información y Servicios Relacionados, mediante resolución de fecha 28 de octubre de 2016.

La infraestructura de clave pública (PKI) de ANF AC sigue las directrices de la Ley No. 67, publicada en el Registro Oficial Suplemento No. 557 de 17 de abril del 2002, de Comercio Electrónico, Firmas y Mensajes de Datos y de su Reglamento General, publicado en el Registro Oficial Suplemento No. 735 de 31 de diciembre de 2002. Y respeta lo establecido en la Constitución de la República de Ecuador, Ley Orgánica de Defensa del Consumidor, Acuerdo Ministerial No 181 de 15 de septiembre de 2011; Acuerdo No 012-2016, y demás que emita el Ministerio de Telecomunicaciones y de la Sociedad de la Información.

El suscriptor y cualquiera que confíe en los certificados electrónicos sometidos a esta Política de Certificación (PC), deberá conocerla, al igual que la Declaración de Prácticas de Certificación (DPC) que marca las prácticas generales de certificación.

En caso de discrepancia, lo estipulado en esta PC prevalecerá sobre lo regulado en la DPC.

Esta PC, es publicada y permanentemente actualizada en,

https://www.anf.ec

ANF AC adecua sus servicios a los siguientes estándares de referencia:

- RFC 3647 (Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework)
- RFC 3739 (Internet X.509 Public Key Infrastructure: Qualified Certificates Profile)
- RFC 5280 (Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile)
- RFC 6960 (X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP)
- RFC 3161 (Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP))
- RFC 3628 (Policy Requirements for Time-Stamping Authorities (TSAs))
- ETSI EN 319 401 (General Policy Requirements for Trust Service Providers)
- ETSI EN 319 411-1 (Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements)
- ETSI EN 319 411-2 (Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates)
- ETSI EN 319 412-1 (Certificate Profiles; Part 1: Overview and common data structures)
- ETSI EN 319 412-2 (Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons)
- ETSI EN 319 412-3 (Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons)
- ETSI EN 319 412-4 (Certificate Profiles; Part 4: Certificate profile for web site certificates)
- ETSI EN 319 412-5 (Certificate Profiles; Part 5: QCStatements)
- A la versión actual de los *Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates* publicados en https://cabforum.org/baseline-requirements-documents/. En caso de incompatibilidad entre este documento y los requisitos, los requisitos tomarán prioridad

sobre este documento, siempre y cuando, estos requisitos no entren en contradicción con normas legales.
- A la versión actual de los *CA/Browser Forum Guidelines for Issuance and Management of Extended Validation Certificate* publicados en https://cabforum.org/extended-validation/. En caso de incompatibilidad entre este documento y los requisitos, los requisitos tomarán prioridad sobre este documento, siempre y cuando, estos requisitos no entren en contradicción con normas legales.
- ISO/IEC 27001 (Information technology - Security techniques - Information security management systems Requirements)
- ISO 9001:2015 (Sistema de Gestión de Calidad para CAs)
- ISO 14001 (Gestión Medioambiental)

ANF AC tiene asignado el código privado de empresa *(SMI Network Management Private Enterprise Codes)* 37442 por la organización internacional IANA -Internet Assigned Numbers Authority-, bajo la rama iso.org.dod.internet.private.enterprise *(1.3.6.1.4.1 -IANA –Registered Private Enterprise-)*.

Para elaborar su contenido se ha seguido la estructura de la IETF RFC 3647 PKIX, incluyendo aquellos apartados que resultan específicos para este tipo de certificado.

Esta Política de Certificación (PC) cumple con lo dispuesto en la Ley de Comercio Electrónico, Firmas y Mensajes de Datos, establece los requisitos de procedimiento y operacionales a los que está sujeto el uso de estos certificados, y define las directrices que ANF AC utiliza para su emisión, gestión, revocación, renovación y cualquier otro proceso que afecte al ciclo de vida. Se describen los papeles, responsabilidades y relaciones entre el usuario final, ANF AC y terceros de confianza, así como las reglas de solicitud, renovación y revocación que se deben atender.

Este documento es sólo uno de los diversos documentos que rigen la PKI de ANF AC, detalla y complementa lo definido en la Declaración de Prácticas de Certificación (DPC) y su adenda. ANF AC tutela y supervisa que esta PC sea compatible y esté en coherencia con el resto de documentos que ha elaborado.

1.1. Descripción de los certificados

Estos certificados se expiden con un periodo de validez máximo de 5 años, en diferentes soportes y según los niveles de seguridad requeridos:

- **Token de software criptográfico**.
- **Token criptográfico (HSM).** Exclusivamente dispositivos con certificación ISO 15408 EAL 4+ Common Criteria, o su equivalente FIPS..
- **Servicio Centralizado de certificados de firma electrónica**. Con módulo de hardware criptográficos (HSM) con certificación ISO 15408 EAL 4+ Common Criteria, o su equivalente FIPS.

Todos los Certificados emitidos bajo esta política son de conformidad con el estándar X.509 versión 3, y son emitidos con la clasificación de reconocidos.

La comprobación de identidad será realizada por ANF AC, o por una Autoridad de Registro (AR, Tercero Vinculado), en base a documentación original vigente y empleando documentos legalmente aceptados en la República de Ecuador.

La comprobación de la información facilitada por el suscriptor, será realizada por ANF AC.

1.1.1. Certificado Electrónico/digital de Persona Física

Se trata de un certificado en el que el suscriptor será una persona natural. Vincula a su titular los datos de verificación de firma y confirma su identidad.

ANF AC identifica al suscriptor del certificado, de acuerdo con la los artículos 12 y 13 de la Ley de Comercio Electrónico, firmas electrónicas y Mensajes de Datos (Ley No. 2002-67)

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

Persona Física	Software Criptográfico	1.3.6.1.4.1. 37442.4.1
	QSCD	1.3.6.1.4.1. 37442.4.2
	QSCD. Servicio Centralizado	1.3.6.1.4.1. 37442.4.3

1.1.2. Certificado Electrónico/digital de Persona Jurídica, Representante legal o Empleado con relación de dependencia

El sujeto titular del certificado es una persona física que interviene, por apoderamiento notarial, en nombre y representación de una persona jurídica. (literal b, numeral 1.2.1, artículo 1 del Acuerdo Ministerial 181, reformado el 25 de enero de 2015 con Acuerdo Ministerial 006-2015): Son certificados que identifican al suscriptor, como una persona jurídica de derecho público y privado a través de su representación legal o de las personas que actúan en su representación, quieres serán responsables en tal calidad de todo lo que firme dentro de su ámbito de competencia y límites de uso que correspondan.

ANF AC emite los siguientes certificados de identidad:

- **Certificado de Persona Jurídica.**

  Es un certificado en el que la persona jurídica queda identificada como titular del certificado. Vincula a su titular los datos de verificación de firma y confirma su identidad.

- **Certificado de Representante Legal de Persona Jurídica**

Es un certificado en el que la persona jurídica y el representante legal quedan identificados, constando los datos de apoderamiento del representante, y dicho apoderamiento determina el alcance de uso del certificado.

- **Certificado de empleado con relación de dependencia**

  Es un certificado en el que la persona jurídica y el empleado con relación de dependencia quedan identificados. Es la persona jurídica la responsable de establecer el límite de uso y suscribir el correspondiente compromiso formal con su empleado.

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

Persona Jurídica	Software Criptográfico	1.3.6.1.4.1. 37442.5.1
	QSCD	1.3.6.1.4.1. 37442.5.2
	QSCD. Servicio Centralizado	1.3.6.1.4.1. 37442.5.3
Representante Legal de Persona Jurídica	Software Criptográfico	1.3.6.1.4.1. 37442.6.1
	QSCD	1.3.6.1.4.1. 37442.6.2
	QSCD. Servicio Centralizado	1.3.6.1.4.1. 37442.6.3
Empleado con relación de dependencia	Software Criptográfico	1.3.6.1.4.1. 37442.7.1
	QSCD	1.3.6.1.4.1. 37442.7.2
	QSCD. Servicio Centralizado	1.3.6.1.4.1. 37442.7.3

1.1.3. Certificados de Empleado Público

Se trata de un certificado en que el sujeto titular del certificado es un funcionario público que ha sido habilitado por la institución pública para firmar en su nombre y representación.

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

Empleado Público	Software Criptográfico	1.3.6.1.4.1. 37442.8.1
	QSCD	1.3.6.1.4.1. 37442.8.2
	QSCD. Servicio Centralizado	1.3.6.1.4.1. 37442.8.3

1.2. Nombre del documento e identificación

Nombre del documento	Política de Certificación de Certificados de Firma electrónica		
Versión	1.0		
Estado de la política	APROBADO		
OID	1.3.6.1.4.1. 37442.3.1		
Fecha de aprobación	20/03/2020	**Fecha de publicación**	20/03/2020

El significado del OID con el arco "1.3.6.1.4.1.37442.3.1" es el siguiente:

- Iso (1)
- Org (3)
- Dod (6)
- Internet (1)
- Private (4)
- Enterprise (1)
- ANFAC Autoridad de certificación Ecuador, C.A. (37442)
- Política de Certificación (3.1)

1.2.1 Control de cambios

Este documento es revisado al menos una vez al año y siempre que se produzcan cambios en la PKI. En caso de requerirlo, se aplican las actualizaciones necesarias para mantener su adecuación a la PKI de ANF AC.

Para gestionar una administración adecuada, se aplica un control de versionado.

Versión	Cambios	Aprobación	Publicación
1.0	Elaboración PC de ANF AC	20/03/2020	20/03/2020

1.3. Partes de la PKI

Según lo definido en la DPC de ANF AC.

1.4. Ámbito de aplicación

1.4.1. Usos permitidos

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

- Especialmente indicado parar realizar operaciones de firma que requieran no repudio y procesos de identificación ante sistemas informáticos.

1.4.2. Límites de uso de los certificados

De forma general, según lo establecido en la Declaración de Prácticas de Certificación de ANF AC.

De forma específica, cabe reseñar que estos certificado será utilizado por los suscriptores en las relaciones que mantengan con terceros que confían, de acuerdo con los usos autorizados en los campos 'Key Usage' y 'Extended Key Usage' del certificado y en conformidad con las limitaciones de uso que conste en el certificado.

Los certificados emitidos con seudónimo, sólo se podrán utilizar en aquellos procesos de firma que expresamente autoricen el empleo de esta modalidad de identificación.

El uso de las claves y el certificado presupone la aceptación de las condiciones de uso establecidas en la DPC y su adenda.

1.4.3. Usos prohibidos

Según lo definido en la DPC de ANF AC.

1.5. Datos de contacto de la Entidad de Certificación

Según lo definido en la DPC de ANF AC.

1.6. Definiciones y Acrónimos

Según lo definido en la DPC de ANF AC.

2. Repositorios y publicación de la información

2.1. Repositorios

Según lo definido en la DPC de ANF AC.

2.2. Publicación de la información

Según lo definido en la DPC de ANF AC.

2.3. Frecuencia de actualizaciones

Según lo definido en la DPC de ANF AC.

2.4. Controles de acceso a los repositorios

Según lo definido en la DPC de ANF AC.

3. Identificación y Autenticación

3.1. Registro de nombres

3.1.1. Tipos de nombres

El perfil se basa en las recomendaciones IETF RFC 5280 y el estándar ITU-T X.509.

Todos los certificados contienen un nombre distintivo (DN o distinguished name) de la persona física titular del certificado, definido de acuerdo con lo previsto en la Recomendación ITUT X.501 y contenido en el campo Subject, incluyendo un componente CommonName.

El atributo O (Organization), en caso de incluirse, debe hacer referencia en el caso de titulación colegiada: Nombre del Colegio Oficial del que es miembro activo. Adicionalmente, se incluye el número de colegiado separado por el carácter "/". Ej: O = Nombre Colegio / número colegiado.

En el caso de certificados de persona jurídica y de persona física representante legal de persona jurídica, la razón social está incluida en el atributo "organizationName" y el RUC en el atributo "organizationIdentifier"

En el caso de capacitación profesional, puede incluir el nombre de la asociación, gremio o agrupación a la que pertenece. O emisor de la titulación de capacitación profesional. Adicionalmente se puede incluir el número de asociado o agremiado como se especifica en el supuesto anterior.

Las circunstancias personales y atributos de las personas y organizaciones identificadas en los certificados se incluyen en atributos predefinidos en normas y especificaciones técnicas de reconocimiento general.

3.1.2. Guía de cumplimentación de campos específicos

De acuerdo con la RFC 5280, que usa UTF-8[*1] string, puesto que codifica grupos de caracteres internacionales incluyendo caracteres del alfabeto latino con diacríticos ("Ñ", "ñ", "Ç", "ç", "Ü", "ü ", etc.). Por ejemplo, el carácter eñe (ñ), que se representa en unicode como 0x00F1.

Para todas las literales variables:

- Todos los literales se introducen en mayúsculas, con las excepciones del nombre de dominio/subdominio y el correo electrónico que estarán en minúsculas.
- No incluir tildes en los literales alfabéticos
- No incluir más de un espacio entre cadenas alfanuméricas.
- No incluir caracteres en blanco al principio ni final de cadenas alfanuméricas.
- Se admite la inclusión de abreviaturas en base a una simplificación, siempre que no supongan dificultad en la interpretación de la información.

*1 *Para más información ver RFC 2279 mejorada en 3629 (UTF-8, a transformation format of ISO 10646)*

3.1.3. Necesidad de que los nombres sean significativos

Los nombres distintivos deben tener sentido.

3.1.4. Seudónimos o anónimos

No se contempla.

3.1.5. Reglas utilizadas para interpretar varios formatos de nombres

Según lo definido en la DPC de ANF AC.

3.1.6. Unicidad de los nombres

Según lo definido en la DPC de ANF AC.

3.1.7. Resolución de conflictos relativos a nombres y marcas

ANF AC no asume compromiso alguno sobre el uso de marcas comerciales en la emisión de los Certificados expedidos bajo la presente Política de Certificación. ANF AC no está obligada a verificar la titularidad o registro de marcas registradas y demás signos distintivos.

Los suscriptores de certificados no incluirán nombres en las solicitudes que puedan suponer infracción.

No se permite el uso de signos distintivos cuyo derecho de uso no sea propiedad del suscriptor o esté debidamente autorizado.

ANF AC se reserva el derecho de rehusar una solicitud de certificado por causa de conflicto de nombre.

3.2. Validación inicial de la identidad

3.2.1. Prueba de posesión de clave privada

Según lo definido en la DPC de ANF AC.

3.2.2. Autenticación de la identidad del suscriptor

Los certificados emitidos bajo esta Política de Certificación identifican al suscriptor que solicita la emisión del certificado.

El Responsable de Dictámenes de Emisión utilizará los medios oportunos para asegurarse de la veracidad de la información contenida en el certificado. Entre estos medios se cuentan bases registrales externas y la posibilidad de requerir información o documentación complementaria al suscriptor.

Los identificativos fiscales del suscriptor se incorporarán en el certificado. Además, el suscriptor debe de facilitar un número de teléfono móvil y una dirección de correo electrónico de su confianza. La dirección de correo electrónico y el servicio SMS o WhatsApp asociado a su teléfono móvil, tendrán la consideración de buzones autorizados para que ANF AC pueda realizar entregar electrónicas certificadas, incluso doble autenticación en el caso de servicio de certificados 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.

3.3. Renovación de la clave

En el supuesto de renovación de la clave, ANF AC informará previamente al suscriptor sobre los cambios que se hayan producido en los términos y condiciones respecto a la emisión anterior.

Se podrá emitir un nuevo certificado manteniendo la anterior clave pública, siempre que siga considerándose criptográficamente segura.

3.4. Solicitud de revocación

Todas las solicitudes de revocación deben estar autenticadas. ANF AC comprobará la capacidad del suscriptor para tramitar este requerimiento.

4. Requisitos Operacionales

4.1. Interoperabilidad y Seguridad.

4.1.1. Operación y gestión de la Infraestructura de Clave Pública

Las operaciones y procedimientos realizados para la puesta en práctica de esta Política de Certificación se realizan siguiendo los controles requeridos por los estándares reconocidos para tal efecto, describiéndose estas actuaciones en los apartados "Controles de seguridad física, instalaciones, gestión y operacionales" y "Controles de seguridad técnica" de la Declaración General de Prácticas de Certificación de ANF AC.

4.1.2. Interoperabilidad

Los estándares y formato de estos certificados garantiza su futura interoperabilidad con países de la Unión Europea, en particular, con sus Administraciones Públicas.

4.2. Solicitud del certificado

ANF AC sólo admite solicitud de emisión de certificado tramitada por una persona física mayor de edad, con plena capacidad legal de obrar.

El suscriptor deberá cumplimentar el Formulario de Solicitud del certificado asumiendo la responsabilidad de la veracidad de la información reseñada, y tramitarlo ante ANF AC utilizando alguno de los siguientes medios:

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.

4.3. Procedimiento de tramitación

4.3.1. Autenticación de identidad

4.3.1.1. Tramitación en el despacho de ARR o OVP

Cuando la tramitación se realice de forma presencial en el despacho de una Autoridad de Registro Reconocida (ARR) o una Oficina de Verificación Presencial (OVP), el suscriptor deberá acreditar su identidad y datos de filiación personal mediante documentación legalmente suficiente. Como mínimo se acreditará:

a) Dirección física y otros datos que permitan contactar con él. Para acreditar la dirección física, se podrán solicitar, a criterio del RDE, facturas de agua, luz, gas centralizado, televisión por cable, celular o Internet, en las que conste la identidad del suscriptor/solicitante y la dirección física. Si esos suministros figuran a nombre del arrendador se podrá acreditar presentando el contrato de arrendamiento, debidamente registrado. Si la ARR o el RDE lo consideran necesario, pueden solicitar documentos adicionales para cotejar la fiabilidad de la información. Si la ARR o el RDE conocen de forma personal al suscriptor deberán emitir y firmar una Declaración de Identidad[1].
b) Según criterio del ARR, OVP, o del RDE, se podrá requerir una o varias evidencias que acrediten la intervención personal del/los interesado/dos, las cuales quedarán asociadas al formulario de solicitud, P.ej. firma manuscrita, firma grafo métrica fotografía, o video, o voz, o huellas dactilares.
c) Cédula de identidad o pasaporte en caso de ciudadanos nacionales, cuya fotografía permita cotejar la identidad de la persona compareciente. En caso de escasa nitidez se podrá solicitar otro documento oficial que incorpore fotografía de mayor calidad (p.ej., licencia de conducir).
d) En caso de ciudadanos extranjeros, se requerirá pasaporte. En caso de escasa nitidez se podrá solicitar otro documento oficial que incorpore fotografía de mayor calidad (p.ej., licencia de conducir).

e) En caso de que el suscriptor disponga de un mandato de representación o un poder notarial, y solicite que ese documento sea adjuntado al certificado. Se requerirá:
    1. **Mandato de representación**. El documento debe de estar en formato pdf y firmado por el mandante, empleando un certificado cualificado de firma electrónica expedido por ANF AC. La solicitud de inclusión del mandato supone para el suscriptor la aceptación plena del mandato de representación.
    2. **Poder notarial**. El documento original será digitalizado por el operador AR el cual lo firmará electrónicamente.

[1] ***Declaración de Identidad**: 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.

f) En el caso de certificados de persona jurídica y representación se deberá presentar original o copia auténtica de la siguiente documentación vigente:

1. **Según forma jurídica**:
   - Sociedades mercantiles y demás personas jurídicas cuya inscripción sea obligatoria en el Registro Público Oficial acreditarán la válida constitución mediante la aportación de original o copia auténtica del Registro Público Oficial relativo a los datos de constitución y cargos vigentes de administración de la entidad.
   - Asociaciones, Fundaciones y Cooperativas acreditarán la válida constitución mediante la aportación de original o copia auténtica de un certificado del Registro Público Oficial donde consten inscritas, relativo a su constitución.
   - Sociedades civiles y demás personas jurídicas aportarán original o copia auténtica del documento que acredite su constitución de manera fehaciente.
   - 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.

2. **Documentación que acredite la válida constitución de la entidad:**

   Certificados o notas simples acreditativos de la inscripción, expedidos en la fecha de la solicitud o en los quince días anteriores, en particular:
   - Tratándose de fondos de inversión, fondos de capital-riesgo, fondos de regulación del mercado de títulos hipotecarios, fondos de titulación hipotecaria, fondos de titulación de activos, fondos de garantía de inversiones y fondos de pensiones: certificado de inscripción en el registro correspondiente del Ministerio de Economía y Hacienda o de la Comisión Nacional del Mercado de Valores, deberá constar en el certificado la identificación de la entidad gestora del fondo.
   - Tratándose de uniones temporales de empresas que se hayan acogido al régimen fiscal especial, y si estuvieran inscritas en el Registro especial de Uniones Temporales de Empresas del Ministerio de Economía y Hacienda, adscrito a la Agencia Estatal de Administración Tributaria, aportarán certificado de dicha inscripción. En el caso de no estar inscritas, documento suscrito por una mayoría de miembros o socios, en el que certifican la vigencia de la entidad.
   - Cuando la entidad no corresponda a ninguna de las tipologías anteriormente reseñadas y, por lo tanto, no deba de estar inscrita en ninguno de esos registros, se presentarán junto con la solicitud los documentos que posea al

respecto el suscriptor, siendo el Responsable de Dictámenes de Emisión el que determine la suficiencia o insuficiencia de los mismos.

g) En el caso de que el suscriptor solicite incluir otras circunstancias personales como su condición de titular de un cargo público, su pertenencia a un colegio profesional o su titulación, éstas deberán comprobarse mediante los documentos oficiales que las acrediten, de conformidad con su normativa específica.

4.3.1.2. Tramitación por legitimación de firma por notario público o compulsa por operador ARR u OVP

Se realzará el siguiente procedimiento:

a) ANF AC pone a disposición del suscriptor políticas de certificación, precios y el formulario de solicitud y el contrato de prestación de servicios de certificación, así como los medios técnicos para que realice la tramitación de solicitud: cumplimentar formulario de solicitud y facilitar documentos acreditativos e identidad y filiación personal.
   Los documentos requeridos para la acreditación serán los mismos que los requeridos en la tramitación ante ARR y OVP.
b) El suscriptor, en su caso, estampa su firma manuscrita o firma grafo-métrica (biométrica) en los documentos correspondientes al trámite de solicitud del certificado.
c) Cumplido este trámite, ANF AC pone a disposición del suscriptor los medios técnicos necesarios para llevar a cabo la generación de su par de claves, selección de PIN (datos de activación de firma), y generación del certificado de petición (CSR bajo estándar PKCS#10).
d) La firma del formulario de solicitud y el contrato de prestación de servicios, será legitimada por conocimiento de firma por notario público o compulsada por un operador OVP o ARR.”

4.3.2. Aprobación o rechazo de las solicitudes de certificados

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 esta Política de Certificación.

Además, 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.

- 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 y generará un incidente informando al Responsable de Seguridad, a fin de determinar la inclusión o no del suscriptor en la lista negra de personas y entidades con OID 1.3.6.1.4.1.37442.56.2.1.

El procedimiento de validación según tipo de certificado es:

- El RDE comprobará la documentación aportada por el suscriptor y por la Autoridad de Registro.
- En el proceso de validación intervendrán dando soporte el Departamento Jurídico y el Departamento Técnico, que revisará y validará técnicamente el certificado de petición PKCS#10.
- En el proceso de comprobación de la información y documentación recibida, se podrán utilizar los siguientes medios:
  - Consulta a los registros públicos oficiales en los que deba estar inscrita la entidad a efectos de comprobar existencia, vigencia de cargos y otros aspectos legales, como actividad y fecha de constitución.
  - Boletines Oficiales de ámbito nacional o regional de los organismos públicos a los que pertenecen organismos y empresas públicas.
- Se verifica que ninguna de las personas físicas asociadas a la solicitud consta en la lista negra de personas y entidades 1.3.6.1.4.1. 37442.56.2.1.

4.3.3. Tiempo para procesar la emisión de certificados

La emisión de un certificado implica la aprobación final y completa de una solicitud por parte del Responsable de Dictámenes de Emisión. La emisión de certificado debe realizarse en un plazo máximo de 48 horas, una vez emitido el informe del RDE según lo definido en la DPC de ANF AC.

4.4. Emisión del certificado

Según lo definido en la DPC de ANF AC. ANF AC evitará generar certificados que caduquen con posterioridad a los certificados de la CA que los emitió.

4.4.1. Acciones de la Entidad de Certificación durante el proceso de emisión

Según lo definido en la DPC de ANF AC.

Una vez emitido el certificado electrónico, la entrega del certificado siempre se realiza de forma telemática. Se debe emplear el mismo dispositivo criptográfico que el suscriptor utilizó para la generación del par de claves criptográficas y el certificado de petición PKCS#10.

El dispositivo criptográfico establece conexión segura con los servidores de confianza de ANF AC. El sistema, de forma automática, realiza las correspondientes comprobaciones de seguridad. En caso de confirmación, el certificado es descargado e instalado automáticamente.

4.4.2. Notificación al suscriptor

ANF AC, mediante correo electrónico, notifica al suscriptor la emisión y publicación del certificado.

4.5. Aceptación del certificado

4.5.1. Aceptación

Según lo establecido en la Declaración de Prácticas de Certificación de ANF AC.

4.5.2. Devolución

El suscriptor dispone de un periodo de 7 días, desde la entrega del certificado, para comprobar el correcto funcionamiento del mismo.

En caso de defectos de funcionamiento por causas técnicas o por errores en los datos contenidos en el certificado, el suscriptor o el responsable del certificado puede mandar un email firmado electrónicamente a ANF AC, informando del motivo de la devolución.

ANF AC verificará las causas de devolución, revocará el certificado emitido y procederá a emitir un nuevo certificado en un plazo máximo de 72 horas.

4.5.3. Seguimiento

ANF AC no es responsable de la monitorización, investigación o confirmación de la exactitud de la información contenida en el certificado con posterioridad a su emisión. En el caso de recibir información sobre la inexactitud o la no aplicabilidad actual de la información contenida en el certificado, este puede ser revocado.

4.5.4. Publicación del certificado

El certificado es publicado en los repositorios de ANF AC, en un plazo máximo de 24 horas desde que se ha producido su emisión.

4.5.5. Notificación de la emisión del certificado a terceros

No se efectúa notificación a terceros.

4.6. Denegación

Según lo establecido en la Declaración de Prácticas de Certificación de ANF AC.

4.7. Renovación de certificados

Con carácter general, según lo establecido en la Declaración de Prácticas de Certificación de ANF AC.

4.7.1. Certificados vigentes

ANF AC notifica por correo electrónico al suscriptor la caducidad del certificado, remitiendo el formulario de solicitud, con el objetivo de proceder a su renovación. Estas notificaciones se envían con 90, 30 y 15 días de antelación a la fecha de caducidad del certificado.

Sólo los certificados en estado de vigencia pueden ser renovados siempre que la identificación realizada no haya superado el periodo de cinco años.

4.7.2. Personas autorizadas para solicitar la renovación

El formulario de solicitud de renovación debe ser firmado por el propio suscriptor o por representante con poder suficiente. Las circunstancias personales del suscriptor no deben haber variado.

4.7.3. Identificación y autenticación de las solicitudes de renovación rutinarias

La identificación y autenticación para la renovación del certificado se puede realizar bien presencialmente, utilizando alguno de los medios descritos en esta sección, o bien tramitando la solicitud de renovación telemáticamente cumplimentando el formulario correspondiente y firmándolo electrónicamente con un certificado vigente emitido con la calificación de "reconocido", y en el que figure como titular el suscriptor del certificado del que se solicita renovación.

ANF AC aplica los siguientes procedimientos y medidas de seguridad técnicas:

- Los certificados de ANF AC siempre se generan utilizando la tecnología necesaria para poder realizar cualquier trámite de renovación, incluso los certificados electrónicos de firma electrónica centralizada.
- ANF AC sigue un sistema de registro de solicitudes, distinguiendo la fecha de solicitud -que coincide con la de identificación- y la de emisión del certificado. El sistema técnico requiere una petición expresa del usuario, la intervención directa de un operador de ANF AC el cual, a su vez, precisa validar la solicitud mediante aplicación de control de seguridad de coherencia.

4.7.4. Aprobación o rechazo de las solicitudes de renovación

Se seguirá el mismo procedimiento que el realizado en el proceso de emisión especificado en este documento.

4.7.5. Notificación de la renovación del certificado

Se seguirá el mismo procedimiento que el realizado en el proceso de emisión especificado en este documento.

4.7.6. Aceptación de la renovación del certificado

Se seguirá el mismo procedimiento que el realizado en el proceso de emisión especificado en este documento.

4.7.7. Publicación del certificado renovado

Se seguirá el mismo procedimiento que el realizado en el proceso de emisión especificado en este documento.

4.7.8. Notificación a otras entidades

Según lo especificado en el apartado 4.4.5 "Notificación de la emisión del certificado a terceros".

4.7.9. Identificación y autenticación de las solicitudes de renovación de clave después de una revocación -Clave no comprometida-

No se autoriza la renovación de certificados caducados, ni revocados.

4.8. Modificación del certificado

No es aplicable.

4.9. Revocación y suspensión de certificados

Con carácter general según lo establecido en la Declaración de Prácticas de Certificación de ANF AC.

4.9.1. Causas de revocación

Además de lo previsto en la Declaración de Prácticas de Certificación, ANF AC:

- Facilitará instrucciones y dará soporte jurídico para la presentación de denuncias o sospechas de compromiso de la clave privada, del mal uso de certificados o cualquier tipo de fraude, o conducta impropia.
- 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:
  - La naturaleza de la incidencia.
  - Informaciones recibidas.
  - Normas legales y regulación sobre la que se fundamente la orden de revocación.

4.9.2. Identificación y autenticación de solicitudes de revocación

Podrán solicitar la revocación de un certificado:

- El suscriptor del certificado.
- El representante del suscriptor con poder suficiente.
- ANF AC.
- La Autoridad de Registro Reconocida que intervino en la tramitación de la solicitud de emisión del certificado.

La política de identificación para las solicitudes de revocación acepta los siguientes métodos de identificación:

- **Telemática**: mediante la firma electrónica de la solicitud de revocación por parte del suscriptor del certificado o del responsable del mismo en la fecha de la solicitud de revocación.
- **Telefónica**: mediante la respuesta a las preguntas realizadas desde el servicio de soporte telefónico disponible en el número +593 02 3826877
- **De forma presencial**: personándose el suscriptor o el representante con poder bastante del titular del certificado en las oficinas de ANF AC, sitas en Av. 12 de Octubre N24-739 y Av. Colón. Edificio Torre Boreal, Torre A, Piso 6. Oficina 603; acreditando su identidad mediante documentación original, y firmando de forma manuscrita el formulario correspondiente.

ANF AC, o cualquiera de las Autoridades de Registro Reconocidas que componen su Red Nacional de Proximidad, pueden solicitar de oficio la revocación de un certificado si tuvieran conocimiento o sospecha del compromiso de la clave privada asociada al certificado, o de cualquier otro hecho que recomendara emprender dicha acción.

ANF AC deberá autenticar las peticiones e informes relativos a la revocación de un certificado, comprobando que provienen de una persona autorizada.

Dichas peticiones e informes serán confirmados cumpliendo los procedimientos establecidos en la Declaración de Prácticas de Certificación.

4.9.3. Procedimiento para la solicitud de revocación

El suscriptor de la Revocación debe cumplimentar el Formulario de Solicitud de Revocación y tramitarlo ante ANF AC por cualquiera de los medios que están previstos en este documento.

La solicitud de revocación deberá contener, como mínimo, la siguiente información:

- Fecha de solicitud de la revocación.
- Identidad del suscriptor.
- Razón detallada de la petición de revocación.
- Nombre y título de la persona que pide la revocación.
- Información de contacto de la persona que pide la revocación.

La solicitud de revocación será procesada a su recepción.

La solicitud tiene que estar autenticada, de acuerdo con los requisitos establecidos en la sección correspondiente de esta política, antes de proceder a la revocación.

Una vez autenticada la petición, ANF AC podrá revocar directamente el certificado e informar al suscriptor y, en su caso, al responsable del certificado sobre el cambio de estado del certificado.

4.9.4. Periodo de gracia de la solicitud de revocación

Según lo definido en la DPC de ANF AC.

4.9.5. Plazo máximo de procesamiento de la solicitud de revocación

Según lo definido en la DPC de ANF AC.

4.9.6. Requisitos de comprobación de listas CRL

Los terceros que confían deben comprobar el estado de los certificados en los cuales van a confiar. Para ello pueden consultar la última CRL emitida dentro del periodo de vigencia del certificado de interés.

4.9.7. Frecuencia de emisión de CRL

Según lo definido en la DPC de ANF AC.

4.9.8. Disponibilidad de comprobación on-line de la revocación

ANF AC pone a disposición de los terceros que confían un servicio on-line de comprobación de revocaciones, el cual está disponible las 24 horas del día, los 7 días de la semana.

4.9.9. Requisitos de la comprobación on-line de la revocación

Los terceros que confían pueden comprobar de forma on-line la revocación de un certificado a través del sitio web https://www.anf.ec

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

Este servicio cumple los requerimientos establecidos en materia de Protección de Datos de Carácter Personal, y únicamente suministra copia de estos certificados a terceros debidamente autorizados.

El acceso a este sistema de consulta de certificados es libre y gratuito.

4.9.10. Suspensión del certificado

No es aplicable.

4.9.11. Identificación y autenticación de solicitudes de suspensión

No está permitida la suspensión del certificado.

4.10. Depósito y recuperación de claves

Salvo en certificados de firma electrónica centralizada, ANF AC no almacena, ni tiene la posibilidad de almacenar la clave privada de los suscriptores y, por lo tanto, no presta servicio de recuperación de claves.

5. Controles de seguridad física, instalaciones, gestión y operacionales

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

a) Control y Detección de Incidentes

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

- Por teléfono: +593 02 3826877
- Por correo electrónico: info@anf.ec
- Cumplimentando el formulario electrónico disponible en el sitio web https://www.anf.ec
- Mediante personación en una de las oficinas de las Autoridades de Registro Reconocidas.
- Mediante personación en las oficinas de ANF AC.

El protocolo de auditoría interna anual requiere específicamente la realización de una revisión de la operativa de emisión de los certificados, con una muestra mínima del 3% de los certificados emitidos.

b) Registro de Incidentes

ANF AC dispone de un Registro de Incidentes en el que se inscribe toda incidencia que se haya producido con los certificados emitidos, y las evidencias obtenidas. Estos incidentes se registran, analizan y solucionan según los procedimientos del Sistema de Gestión de la seguridad de la Información de ANF AC.

El Responsable de Seguridad determina la gravedad del incidente y nombra un responsable y, en caso de incidentes de seguridad relevantes, informa a la Junta Rectora de la PKI.

5.1. Controles de seguridad física

Según lo definido en la DPC de ANF AC.

5.2. Controles de procedimiento

Según lo definido en la DPC de ANF AC.

5.3. Controles de personal

Según lo definido en la DPC de ANF AC.

6. Controles de seguridad técnica

Según lo definido en la DPC de ANF AC.

7. Perfiles de certificados, listas 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).*

Los certificados emitidos con la calificación de cualificados, cumplen con las normas:

- ETSI EN 319 412 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements.
- RFC 3739 Internet X.509 Public Key Infrastructure: Qualified Certificates Profile.

El periodo de validez del certificado está reseñado en Tiempo Coordinado Universal, y codificado conforme a la especificación RFC 5280.

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

Dentro de los certificados, además de los campos comunes ya estandarizados, se incluyen un conjunto de campos "propietarios" que aportan información relativa al suscriptor, u otra información de interés.

Campos propietarios

Se han asignado identificadores unívocos a nivel internacional. Concretamente:

- Los campos referenciados con el identificador de objeto (OID) 1.3.6.1.4.1.37442.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.

QCStatements

Los certificados emitidos por ANF AC, con el fin de garantizar una futura interoperabilidad con países miembros de la Unión Europea, siguen lo definido en la ETSI EN 319 412-5 *(Certificate Profiles-QCStatements)*:

- **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 (reconocido)".

- **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. DÓLARES AMERICANOS 100x10 elevado a 1, lo que presupone límite monetario de 1000 DÓLARES AMERICANOS.

  Además, con el fin de facilitar la consulta de esta información, el límite de responsabilidad se incluye en la extensión propietaria del OID 1.3.6.1.4.1.37442.41.1, 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. 37442.41.1
- **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.
- **QcType**, cuando el certificado se emite con el perfil (FIRMA), se reseña QcType 1
- **QcPDS**, se proporciona la URL que permite acceder a todas las políticas de la PKI en inglés. De acuerdo con ETSI 319 412-5 se utilizará protocolo https.

SubjectAlternativeNames

La especificación IETF RFC 5280 prevé el empleo de los siguientes tipos de datos:

- Identidad basada en correo electrónico.
- Identidad basada en nombre diferenciado (DN), que se suele emplear para construir un nombre alternativo basado en atributos propietarios, que no resultan ambiguos en ningún caso.
- Identidad basada en nombre de dominio de Internet (DNS).
- Identidad basada en dirección IP.
- Identidad basada en identificador de recurso universal (URI).
-

7.1. Perfiles de certificados

Según lo definido en el documento perfil técnico.

7.2. Perfil de CRL

Según lo definido en la DPC de ANF AC, y documento perfil técnico.

7.3. Perfil de OCSP

Según lo definido en la DPC de ANF AC, y documento perfil técnico.

8. Auditoría de conformidad

Según lo definido en la DPC de ANF AC.

9. Disposiciones generales

Según lo definido en la DPC de ANF AC.