Declaración de Prácticas de Certificación (DPC)

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

Documento Público

Aviso Importante

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

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, su Reglamento General, publicado en el Registro Oficial Suplemento No. 735 de 31 de diciembre de 2002, el Decreto núm. 1356, de 29 de septiembre de 2008, de Reforma del Reglamento General y la Resolución ARCOTEL-2024-0176, de fecha 16 de agosto de 2024, por la que se expide la "NORMA TÉCNICA PARA LA PRESTACIÓN DE LOS SERVICIOS DE INFORMACIÓN Y SERVICIOS RELACIONADOS DE LAS ENTIDADES DE CERTIFICACIÓN ACREDITADAS Y TERCEROS VINCULADOS",

Así mismo, respeta lo establecido en la Constitución de la República de Ecuador y en la Ley Orgánica de Defensa del Consumidor.

Esta DPC, sus políticas y adenda, están publicadas en la web corporativa de ANF AC

https://www.anf.ec

ANF AC Ecuador es filial de ANF AC España, Prestador Cualificado de Servicios de Confianza acreditado conforme al Reglamento [UE] 910/2014, de 23 de julio de 2014, del Parlamento Europeo y del Consejo (eIDAS), modificado por el Reglamento (UE) 2024/1183 del Parlamento Europeo y del Consejo, de 11 de abril de 2024, por el que se modifica el Reglamento (UE) nº 910/2014 en lo que respecta al establecimiento del marco europeo de identidad digital (eIDAS 2)

ANF AC Ecuador, cuenta con el apoyo técnico y logístico de ANF AC España en el desarrollo de su actividad como Entidad de Certificación de Información y Servicios Relacionados.

1.1. Visión general

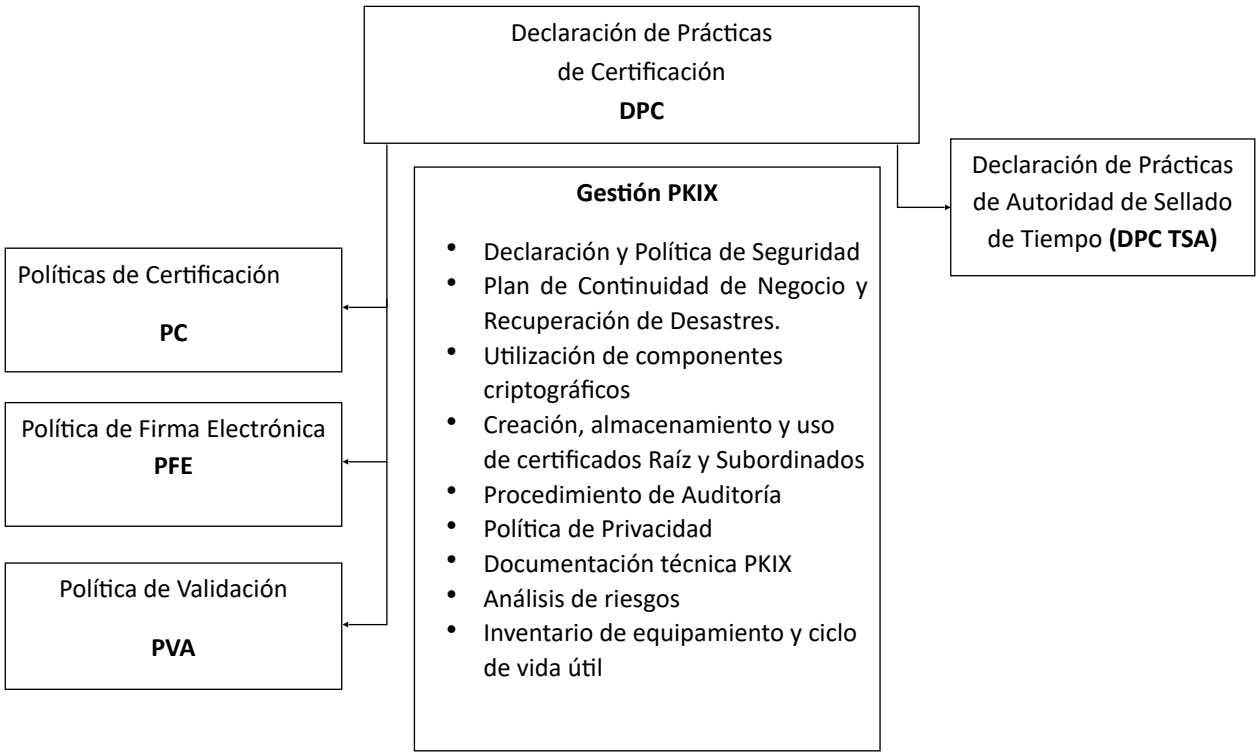
El presente documento es la Declaración de Prácticas de Certificación (DPC) de ANF AC. Este documento detalla los medios y procedimientos que ANF AC emplea para atender los requerimientos y niveles de seguridad impuestos para los diversos tipos de certificados que emite, en sus respectivas Políticas de Certificación.

Las condiciones de uso, limitaciones, responsabilidades, propiedades y cualquier otra información que se considere específica de cada tipo de certificado, viene reflejada en cada una de estas Políticas de Certificación a las que se somete su respectiva emisión. El suscriptor de cualquier tipo de certificado ha de conocer esta DPC y la PC que en cada caso le sea de aplicación para poder solicitar y usar de forma correcta el certificado electrónico y los servicios de confianza prestados por ANF AC. Lo estipulado en las Políticas de Certificación específicas prevalecerá sobre lo regulado en esta DPC. Pueden encontrarse publicadas en la web corporativa de ANF AC

https://www.anf.ec

De acuerdo con el artículo 5.1 de la Resolución ARCOTEL-2024-0176, de 16 de agosto de 2024, esta DPC detalla las normas y condiciones generales de los servicios de certificación de ANF AC en relación con la gestión de los datos de creación y verificación de firma y de los certificados electrónicos; las condiciones aplicables a la solicitud, expedición, uso, suspensión y extinción de la vigencia de los certificados; las medidas de seguridad técnicas y organizativas; los perfiles y los mecanismos de información sobre la vigencia de los certificados; y en especial los procesos de comprobación a los que se someten los datos facilitados por los suscriptores de certificados, a fin de determinar su veracidad. También, en esta DPC y en las PC relacionadas se establece la delimitación de responsabilidades de las diferentes partes intervinientes, así como las limitaciones de las mismas ante posibles daños y perjuicios.

La estructura documental de las Políticas, Declaración de Prácticas de Certificación y otros documentos relacionados con los servicios de certificación gestionados por ANF AC, queda descrita en el siguiente esquema:



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

- 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)
- En 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.
- En 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.

Esta Declaración de Prácticas de Certificación está estructurada siguiendo la especificación del estándar RFC 3647 (*Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework*), y 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.

1.2. Nombre del documento e identificación

Nombre del documento	Declaración de Prácticas de Certificación de ANF AC
Versión	3.0
Estado de la política	APROBADO
OID	1.3.6.1.4.1.37442.1.9.1.1
Fecha de aprobación	25/07/2025
Fecha de publicación	25/07/2025
Localización	https://www.anf.ec

1.2.1. Revisiones

Versión	Cambios	Aprobación	Publicación
3.0	Adaptación a la Resolución ARCOTEL-2024-0176, de 16 de agosto de 2024	25/07/2025	25/07/2025
2.0	Mejora de procedimientos PKI	19/05/2020	19/05/2020
1.0	Inicial	28/10/2016	28/10/2016

1.2.2. OIDs

ANF AC utiliza identificadores de objeto OID, según el estándar ITU-T Rec. X.660 y el estándar ISO/IEC 9834-1:2005. 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. El significado del arco OID "1.3.6.1.4.1.37442" es:

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

Con el objeto de identificar de forma individual cada tipo de certificado emitido de acuerdo con la presente DPC y PC a la que está sometido, se asigna un OID. Este OID aparece en la sección correspondiente del "Certificate Policies").

ANF AC emite los siguientes tipos de certificados:

Tipo	Soporte	OID
Certificado de Persona Natural	En archivo (Software Criptográfico)	1.3.6.1.4.1.37442.2.1.1
	En Dispositivos Seguros de Creación de Firma (DSCF)	1.3.6.1.4.1.37442.2.1.2
Certificado de Miembro de Empresa	En archivo (Software Criptográfico)	1.3.6.1.4.1.37442.2.2.1
	En Dispositivos Seguros de Creación de Firma (DSCF)	1.3.6.1.4.1.37442.2.2.2
Certificado de Representante Legal	En archivo (Software Criptográfico)	1.3.6.1.4.1.37442.2.3.1
	En Dispositivos Seguros de Creación de Firma (DSCF)	1.3.6.1.4.1.37442.2.3.2
Certificado de Sello Electrónico	En archivo (Software Criptográfico)	1.3.6.1.4.1.37442.2.4.1
	En Dispositivos Seguros de Creación de Firma (DSCF)	1.3.6.1.4.1.37442.2.4.2

Las especificidades relativas a cada tipo de certificado, según su OID, están reguladas en la Política específica para cada certificado publicadas en la web corporativa de ANF AC.

Los mecanismos de identificación ofrecidos por ANF AC están definidos siguiendo las directrices de la Resolución ARCOTEL-2024-0176, de fecha 16 de agosto de 2024, por la que se expide la "NORMA TÉCNICA PARA LA PRESTACIÓN DE LOS SERVICIOS DE INFORMACIÓN Y SERVICIOS RELACIONADOS DE LAS ENTIDADES DE CERTIFICACIÓN ACREDITADAS Y TERCEROS VINCULADOS"

1.3. Participantes de la PKI

1.3.1. Autoridad de Certificación (CA) o Entidad de Certificación de Información y Servicios Relacionados.

ANFAC AUTORIDAD DE CERTIFICACION ECUADOR C.A., en adelante, ANF AC, con domicilio en Av. 12 de Octubre N24-739 y Av. Colón. Edificio Torre Boreal, Torre A, Piso 6. Oficina 603 y RUC 1792601215001, es una Entidad de Certificación de Información y Servicios Relacionados.

También denominada Autoridad de Certificación (AC o CA “Certification Authority”), según Ley Modelo de la Comisión de la Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI) sobre las Firmas Electrónicas UNCITRAL.

ANF AC dispone de una jerarquía de CAs que conforman su infraestructura de clave pública, y garantiza que éstas cumplen con los requisitos normativos, tanto los técnicos como jurídicos, y con lo establecido en esta DPC y su adenda.

La CA puede hacer uso de otras partes para proporcionar los servicios de certificación. Sin embargo, la CA siempre mantiene la responsabilidad general y garantiza que se cumplen los requisitos normativos, tanto técnicos como jurídicos.

ANF AC dispone de las siguientes Autoridades de Certificación Raíz e Intermedias:

1.3.1.1. Autoridades de Certificación Raíz (Root CA)

ANF AC cuenta en la actualidad con las siguientes Autoridades de Certificación Raíz:

ANF High Assurance Ecuador Root CA, fecha de caducidad 10 de diciembre de 2039, con los siguientes datos de identificación:

ANF High Assurance Ecuador Root CA			
Sujeto	CN = ANF High Assurance Ecuador Root CA	**Serial number**	102547609442997025
	SERIALNUMBER=1792601215001		
	O = ANFAC AUTORIDAD DE CERTIFICACION ECUADOR C.A.	**Clave Pública**	RSA (4096 Bits)
	C = EC	**Algoritmo de firma**	Sha256RSA
Periodo de vigencia	Válido desde el 17/10/2019 hasta el 12/10/2039		
Fingerprint SHA-256	0f361d8b258123ea9bb84dd3f2c821c0285479626e1185e12f1a04b85546e459		

ANF AC Ecuador Root CA, fecha de caducidad 4 de octubre de 2044, con los siguientes datos de identificación:

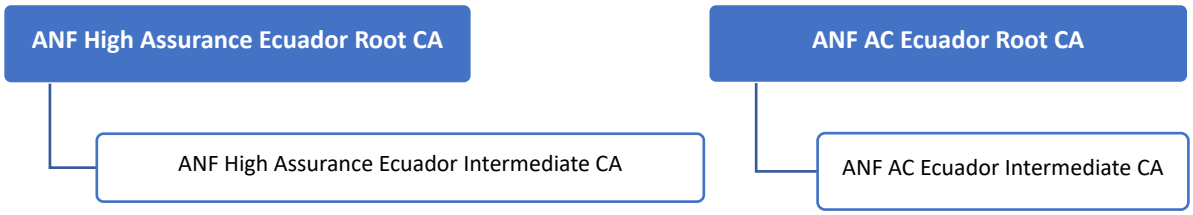
ANF AC Ecuador Root CA			
Sujeto	CN = ANF AC Ecuador Root CA	**Serial number**	997415897105898611376721711
	SERIALNUMBER = 1792601215001		
	O = ANFAC AUTORIDAD DE CERTIFICACION ECUADOR C.A.	**Clave Pública**	RSA (4096 Bits)
	C = EC	**Algoritmo de firma**	Sha256RSA
Periodo de vigencia	Válido desde el 09/10/2024 hasta el 04/10/2044		
Fingerprint SHA-256	2cffd0682dc8354c861b3be82c4a53a2746848192d2d7fc56d33e3be7a291005		

1.3.1.2. Autoridades de Certificación Intermedias (CA IA)

Son las entidades que, dentro de la jerarquía de certificación, emiten certificados de entidad final y cuyo certificado de clave pública ha sido firmado electrónicamente por la Autoridad de Certificación Raíz.

Todas las Autoridades de Certificación Intermedias (CA IA) pueden emitir certificados de Respondedor OCSP. Este certificado es utilizado para firmar y verificar las respuestas del servicio OCSP sobre el estado de los certificados emitidos por estas AC. El OID de los certificados emitidos por cada Autoridad de Certificación Intermedia para la emisión de certificados de respondedor OCSP es 1.3.6.1.4.1.37442.56.1.1

A modo de descripción gráfica de las jerarquías actuales de ANF AC:



ANF High Assurance Ecuador Root CA, con **fecha de caducidad 2039**, cuenta en la actualidad con la siguientes CA Intermedias:

ANF High Assurance Ecuador Intermediate CA			
Sujeto	CN = ANF High Assurance Ecuador Intermediate CA	**Serial number**	102135152490546299
	SERIALNUMBER = 1792601215001	**Clave Pública**	RSA (4096 Bits)
	O = ANFAC AUTORIDAD DE CERTIFICACION ECUADOR C.A.	**Algoritmo de firma**	Sha256RSA
	OU = ANF Autoridad intermedia EC		
	C = EC		
Periodo de vigencia	Válido desde el 17/10/2019 al 14/10/2029		
Comentario	Emite certificados de firma electrónica.		
Fingerprint SHA-256	7d0a3123ce51a38333ed75b0d2d20c877f29671f7b38ac453e0c730b86a8cc9b		

ANF AC Ecuador Root CA, con **fecha de caducidad 2044**, cuenta en la actualidad con las siguientes CA intermedias:

ANF AC Ecuador Intermediate CA			
Sujeto	CN = ANF AC Ecuador Intermediate CA	**Serial number**	0345C5CDEA742EC405553CA7
	OI = VATEC-1792601215001	**Clave Pública**	RSA (4096 Bits)
	O = ANFAC AUTORIDAD DE CERTIFICACION ECUADOR C.A.	**Algoritmo de firma**	Sha256RSA
	C = EC		
Periodo de vigencia	Válido desde el 14/05/2025 hasta el 03/10/2044		
Comentario	Emite certificados cualificados de firma electrónica y de sello electrónico.		
Fingerprint SHA-256	95cb3fa7a322756c2f16f24ddc6728aa12841bd6f98eb74304c7868690c9a1e5		

1.3.2. Terceros Vinculados - Autoridades de Registro

El artículo 33 de la 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 establece que los servicios de certificación de información podrán ser proporcionados y administrados en todo o en parte por terceros. Para efectuar la prestación, éstos deberán demostrar su vinculación con la Entidad de Certificación de Información.

El Decreto núm. 1356, de 29 de septiembre de 2008, de Reforma del Reglamento General sustituyó la denominación "Entidad de Registro" por "Tercero Vinculado".

Así mismo, el Decreto núm. 1356 crea el Registro Público Nacional de Entidades de Certificación de Información y Servicios Relacionados Acreditadas y Terceros Vinculados.

Esta Declaración de Prácticas de Certificación se aplica a los Terceros Vinculados o Autoridades de Registro que ANF AC emplee para atender de forma presencial a los suscriptores de certificados.

Se podrá utilizar de manera indistinta una u otra denominación por identificarse las funciones de los terceros vinculados con las atribuidas internacionalmente a las Autoridades de Registro.

Los terceros vinculados realizan las tareas de identificación de los suscriptores y poseedores de claves de los certificados, comprobación y digitalización certificada de la documentación acreditativa de las circunstancias que constan en los certificados, así como revocación y trámites de renovación de los certificados.

ANF AC desde el inicio de su actividad ha separado la actividad de identificación propiamente dicha, de la valoración de esa identificación. Siendo la única labor ejercida por sus Autoridades de Registro la constatación presencial del suscriptor de los certificados y cotejo de documentos, transmitiendo esa documentación a ANF AC para comprobación y valoración de los documentos y circunstancias requeridos para la emisión de los certificados electrónicos solicitados. Servicio realizado por la figura interna de ANF AC, adscrita a su Departamento Jurídico, denominada *Responsable de Dictámenes de Emisión* (RDE)

Con antelación al inicio de su actividad de autoridad de registro, los Terceros Vinculados a ANF AC habrán suscrito el correspondiente contrato de asunción de responsabilidades y convenio de colaboración.

Los Terceros Vinculados se valen de personas físicas que han realizado el curso de formación de "Operador AR" de ANF AC, y han superado las pruebas de capacitación como "Operador AR"; es un requerimiento preceptivo para el desempeño de estas funciones. Esos Operadores AR son dependiente del Tercero Vinculado, están bajo la supervisión, control y dirección de éste, y son de su exclusiva responsabilidad.

ANF AC encomienda a estos operadores, oficialmente reconocidos, la identificación y comprobación de las circunstancias personales de los suscriptores de certificados.

Con ese objetivo, los operadores:

- Garantizan que el trámite se realiza de forma presencial por parte de las personas implicadas en la solicitud, custodia y uso del certificado solicitado.
- Garantizan que los documentos aportados para la identificación y acreditación de la capacidad de representación son originales y suficientes para llevar a cabo este trámite.
- En la medida de sus posibilidades determinan que el suscriptor, y cuantas personas intervienen en el trámite de solicitud:
    - lo realizan por voluntad propia y sin mediar coacción alguna;
    - son mayores de edad y tienen plena capacidad para obrar;
    - tienen la capacidad intelectual suficiente como para asumir la responsabilidad del correcto uso de los certificados e instrumentos asociados que solicitan.
- Atienden consultas y clarifican dudas sobre todas aquellas cuestiones que al respecto les son formuladas.
- Ponen a disposición del suscriptor, y de todas las personas que intervienen en el trámite de solicitud, la DPC, las Políticas de Certificación asociadas, la Política de Firma Electrónica y las tasas de servicio, así como la información relacionada con el proceso de renovación y de revocación: causas, obligaciones y procedimiento a seguir.
- Informan a los suscriptores de las condiciones precisas para la utilización del certificado y sus limitaciones de uso.
- Verifican que el propietario de los datos presta su consentimiento al tratamiento de sus datos personales, y es informado sobre la finalidad que se les va a dar y su inclusión en el fichero declarado al efecto por ANF AC, así como sobre su derecho de acceso, rectificación, cancelación y oposición, y la forma de ejercerlo.
- Caso de que el certificado vaya a emitirse en un Dispositivo Seguro de Creación de Firma (DSCF), como token o tarjeta criptográfica, hacen entrega de ese dispositivo criptográfico que servirá al suscriptor, entre otras utilidades, para:
    - la generación del par de claves;
    - la generación de los datos de activación;
    - la generación del certificado de petición;

- la conexión con los servidores de confianza de ANF AC mediante protocolo de comunicaciones seguro;
- la descarga del certificado una vez emitido, la generación firmas electrónicas;
- la firma electrónica y la realización de procesos de verificación;
- los procesos de autenticación ante aplicaciones informáticas, y los procesos de cifrado.

Este dispositivo permitirá al usuario el acceso, almacenamiento, control y gestión de sus certificados y claves privadas. Por lo tanto, la destrucción del mismo implica la destrucción del certificado, así como de sus claves.

- Hacen entrega al suscriptor del acta de identificación, firmada electrónicamente por el operador AR.
- Comprueban que toda la documentación presentada por el suscriptor, y cuantas personas intervienen en el trámite de solicitud, es original, obteniendo una copia de los mismos que es firmada electrónicamente por el Operador AR. Esta documentación, junto con el resto de información obtenida y elaborada por el Operador AR (formulario de solicitud, declaración de identidad, datos biométricos…etc.), conforma el "expediente de solicitud". El expediente de solicitud se remite por medios telemáticos a los servidores de confianza de ANF AC.

El proceso de digitalización y transmisión del expediente de solicitud es asumido por la aplicación *AR Manager* de ANF AC, la cual garantiza la seguridad y la privacidad de la información. AR Manager incorpora las siguientes medidas de seguridad:

- El operador AR utiliza un certificado cualificado de firma electrónica emitido a su nombre y sometido a la Política de Certificados AR, para acreditar su identidad ante el programa.
- El operador AR utiliza su certificado cualificado de firma electrónica para autenticar con firma PAdES LT, todos los documentos asociados a la tramitación de solicitud que realiza.
- AR Manager verifica la vigencia del certificado y que el titular es un operador autorizado por ANF AC.
- AR Manager, previa a la aceptación de la transacción realiza validación de las firmas electrónicas elaboradas por el operador AR.
- Se verifica que las direcciones de correo electrónico indicadas tengan el formato correcto. Y se comprueba su validez.
- No se permite que el correo del certificado electrónico sea el mismo que el del Operador AR.
- Se verifica que los RUC indicados tengan el formato correcto.
- Se verifica que los números de las cédulas de identidad indicadas tengan el formato correcto.
- Se verifica que las cuentas bancarias indicadas tengan el formato correcto.
- Se verifica que se adjuntan los documentos mínimos acorde con el tipo de certificado solicitado.
- Todos los campos alfanuméricos aparecen en mayúsculas, a excepción de las direcciones de correo electrónico y las URL.

- No se permite la introducción de espacios en blanco al principio o al final de ningún valor indicado, ni varios espacios en blanco seguidos.

- Al finalizar el trámite de solicitud el Operador AR genera y firma el Acta de Identificación, transfiriendo al Dispositivo Criptográfico de Firma Electrónica, y genera en soporte papel la Carta de Activación, todo ello es entregado al suscriptor del certificado. Estos documentos contienen:

  - El Acta de Identificación incorpora de forma estructurada toda la información que posibilitará al suscriptor elaborar el certificado de petición PKCS#10. El Acta de Identificación previamente es cifrada con doble llave.

  - La Carta de Activación contiene una de las contraseñas necesarias para descifrar el Acta de Identificación. La segunda contraseña será enviada mediante correo electrónico a la cuenta indicada en la solicitud.

- En base a los datos acreditados proceden a:

  - Cumplimentar los formularios de solicitud y el contrato de suscripción.

  - Imprimir los referidos documentos, los cuales serán firmados de forma manuscrita por el operador de la Autoridad de Registro que realiza el trámite y por el suscriptor.

  - Remitir a ANF AC toda la documentación correspondiente a la solicitud tramitada.

  - Generar el acta de identificación.

Una vez formalizados los documentos, se entregará al suscriptor:

- Dispositivo de Generación de Datos de Creación de Firma.
- Dispositivo de Creación de Firma Electrónica.
- Dispositivo de Verificación.
- Acta de Identificación que le permite generar su “certificado de petición”.
- Claves de activación del acta.

El Formulario de Solicitud es un documento en el que el suscriptor acepta una declaración expresa de su conocimiento sobre el uso del Dispositivo de Firma Electrónica y del Certificado Electrónico, así como sus deberes, limitaciones y obligaciones como usuario de los mismos. Las obligaciones contempladas son:

- Generar los datos de creación de firma sin la mediación de terceros y que sólo él conozca la contraseña de activación.
- Entender sus obligaciones de custodia de los datos de creación de la firma y de la contraseña de activación.
- Conocer los medios para la comunicación de la pérdida o posible utilización indebida de datos del certificado y firma electrónica, así como su obligación de revocar el certificado en caso de que eso sucediera.
- Conocer la forma como se utiliza el dispositivo de certificación que se le ha entregado.

Los formularios de solicitud de cada certificado se encuentran recogidos en la página web de ANF AC: https://www.anf.ec

En el caso de entrega de un dispositivo criptográfico que incorpora lector de datos biométricos, el Tercero Vinculado deberá asegurarse de que, en su presencia, el suscriptor procede a identificarse ante el dispositivo con sus huellas

dactilares. Mediante este procedimiento el dispositivo quedará activado y personalizado. Sólo el suscriptor podrá, tras someterse a la verificación biométrica correspondiente, activar el sistema de certificación.

Asimismo, deberá requerir, previa a la formalización de la solicitud de emisión del certificado, que se efectúe una lectura de sus Derechos y Obligaciones, informando sobre las dudas que al respecto pueda tener. No se puede formalizar la solicitud de emisión del certificado hasta que el suscriptor considere que tiene una comprensión plena de los documentos. Con la firma de la solicitud del certificado, el suscriptor reconoce que comprende y acepta todos los Derechos y Obligaciones establecidos en esta PKI.

En cualquier caso, si el operador AR estima que las consultas realizadas por el suscriptor se encuentran fuera del ámbito de sus conocimientos u obligaciones, o bien no logra resolver las dudas que le plantean, instruirá al suscriptor para que contacte con la Oficina de Atención al Cliente de ANF AC y que sea personal especializado de este departamento el que atienda y facilite gratuitamente el asesoramiento requerido.

El Tercero Vinculado asume la obligación de revocar los certificados que haya tramitado o denegar una emisión de certificado en trámite cuando:

- Tenga conocimiento de que las circunstancias del titular o del representante legal, en su caso, han cambiado.
- Tenga conocimiento de que se ha producido un quebranto que afecte a la seguridad de los datos de creación de firma.
- En cualquier supuesto en el que considere que su vigencia puede afectar negativamente a la confiabilidad de la PKI de ANF AC; su uso no esté enmarcado en la buena fe; o se utilice en perjuicio de terceros o en operaciones ilegales.

Los criterios de valoración que seguirá el Tercero Vinculado sobre la documentación aportada por el suscriptor para acreditar identidad u otros datos a incluir en el certificado, serán los normalmente aceptados en Derecho. El Tercero Vinculado siempre exigirá la presencia física del suscriptor.

Todos los trámites realizados por los Terceros Vinculados son firmados electrónicamente por los operadores que los realizan, asumiendo así su plena responsabilidad en el proceso.

Los Terceros Vinculados cuentan con la autorización de cobrar las tasas de identificación, solicitud, activación e inclusión de atributos del certificado solicitado.

La valoración final de la suficiencia o no de la comprobación realizada por el Tercero Vinculado, así como de los documentos aportados, correrá siempre a cargo de personal perteneciente a ANF AC.

Una vez emitido el certificado, el Tercero Vinculado recibe una confirmación de la emisión mediante correo electrónico.

1.3.3. Suscriptores

1.3.3.1. Suscriptor

Son las personas naturales, mayores de edad, con plena capacidad jurídica y de obrar, en nombre propio o en representación de terceros, que solicitan a la Entidad de Certificación la emisión de un certificado y con quien firma el contrato de suscripción. En caso de asumir la representación de un tercero, esta representación tiene que estar sustentada con poder con un alcance suficiente a efectos legales, y en caso de tratarse de la representación de una

persona jurídica, el poder debe de estar inscrito en el registro correspondiente, con las excepciones que marque la legislación vigente.

Se advierte que ANF AC no emite certificados a menores de edad, ni a personas sin plena capacidad jurídica y de obrar.

La Resolución ARCOTEL-2024-0176, de fecha 16 de agosto de 2024 hace alusión al *signatario*, quien, en concordancia con la ETSI EN 319 411, es el suscriptor.

> *"Signatario: Es la persona que posee los datos de creación de la firma electrónica, quien, o en cuyo nombre, y con la debida autorización se consigna una firma electrónica."*

El Suscriptor es responsable ante la CA por el uso de la clave privada asociada con el certificado de clave pública, su identidad será incluida en el certificado y solamente se podrá solicitar la emisión de un certificado en los siguientes supuestos:

a) Para solicitar un certificado de persona física, el suscriptor es:

    i. La misma persona física. Cuando el suscriptor y el sujeto (titular) son la misma persona, éste será directamente responsable del incumplimiento de las obligaciones.

    ii. Una persona física con poderes suficientes para representar a la persona física o jurídica.

b) Para solicitar un certificado de representante legal de persona jurídica o entidad sin personalidad jurídica, el suscriptor es:

    i. Un representante legal de la persona jurídica o entidad sin personalidad jurídica con suficientes poderes.

c) Para solicitar un certificado de sistema, servidor o web, por ejemplo, SSL, el suscriptor es:

    i. La persona física representante legal de la organización interesada.

1.3.3.2. **Sujeto**

La Resolución ARCOTEL-2024-0176, de fecha 16 de agosto de 2024 lo denomina *"Titular de Firma: Es la persona natural o jurídica (pública o privada) a favor de quien se ha emitido un certificado u otorgado un servicio relacionado por parte de una Entidad de Certificación de Información y Servicios Relacionados Acreditada o a través de Tercero Vinculado, por lo tanto, será el propietario del certificado"*

El sujeto puede ser:

a) El Suscriptor en caso de solicitar para sí mismo el certificado.

b) Una persona física a quien el Suscriptor le solicita el certificado actuando como su representante legal.

c) Una persona jurídica, por ejemplo, sello electrónico, a quien el Suscriptor le solicita el certificado.

d) El miembro de empresa o empleado con relación de dependencia, a quien el suscriptor (la empresa u organización) con competencias suficientes de representación, le solicita la emisión del certificado para autenticarse en sus relaciones telemáticas y ser utilizado para la generación de firmas electrónicas como miembro de la empresa o empleado con relación de dependencia.

1.3.4. Terceros que confían

De forma general son todas aquellas personas físicas o jurídicas, entidades u organizaciones, Administraciones Públicas o Corporativas que, de forma voluntaria, confían en los certificados electrónicos, en las firmas electrónicas que generan, servicio firma electrónicas en dispositivo de certificados centralizados de ANF AC, en los sellos de tiempo electrónicos y en los procesos de autenticación que se realizan en el ámbito de esta PKI.

El tercero receptor de certificados o sellos de tiempo, asume su responsabilidad como "tercero que confía" cuando acepta en sus relaciones con los suscriptores el empleo de estos instrumentos.

Cuando se haya dado este uso, el tercero receptor asume la inexistencia de toda declaración por la cual pretenda afirmar no confiar en los certificados, en las firmas electrónicas o sellos de tiempo, asumiendo que confió efectivamente en ellos y, por lo tanto, adquiriendo las responsabilidades y obligaciones correspondientes.

Los "Terceros que confían" han de realizar las operaciones de clave pública de manera satisfactoria para confiar en el certificado, así como asumir la responsabilidad de verificar el estado del certificado, el ámbito de uso autorizado, así como las limitaciones de responsabilidad que consten en los certificados y políticas a las que se someten, para ello deberán utilizar los medios que se establecen en esta DPC y Políticas que conforman su adenda.

Los terceros que confían deben de actuar con base en los principios de buena fe y lealtad, absteniéndose de realizar conductas fraudulentas o negligentes cuyo fin sea repudiar los procesos de identificación o firma electrónica, sello de tiempo, o cualquier tipo de manipulación de los certificados electrónicos.

1.3.5. Responsable de Dictámenes de Emisión

Es personal adscrito al Departamento Jurídico de ANF AC, encargado de comprobar la documentación aportada por los Terceros Vinculados. Determinan la suficiencia o deficiencia de esos documentos, comprueban la fiabilidad de la información aportada por el suscriptor, ordenando, si lo consideran, indagaciones complementarias.

El Responsable de Dictámenes de Emisión determinará en cada caso la necesidad de completar la comprobación, mediante la consulta telemática de los registros directamente o a través de servicios de terceros.

1.3.6. Responsables de Emisión de Certificados

Son un mínimo de tres los operadores que cuentan con la capacidad para acceder y activar los dispositivos de emisión de certificados de ANF AC.

Para activar el servicio de emisión, es necesaria la presencia de al menos dos de estos operadores.

1.3.7. Autoridad de Validación

Una Autoridad de Validación es una Entidad de Certificación que proporciona certeza sobre la validez de los certificados electrónicos.

ANF AC es una Autoridad de Validación (VA o Validation Authority) que actúa como tercera parte de confianza validando certificados electrónicos.

ANF AC gestiona un sistema informático formado por un conjunto de Servidores de Confianza, que acceden en tiempo real al estado en que se encuentran todos los certificados emitidos por ANF AC.

Estos servidores reciben el nombre de OCSP Responder y atienden peticiones de validación mediante el protocolo Online Certificate Status Protocol (OCSP). Tienen como función determinar el estado actual de un certificado electrónico y toda su cadena de confianza, emitiendo informe cualificado de validación. Los repositorios a los que acceden los servidores OCSP Responder están permanentemente actualizados, y cumplen la IETF 6960, Online Certificate Status Protocol Algorithm Agility.

Las consultas OCSP pueden ser realizadas bajo régimen 24x7x365 de manera gratuita. Estas consultas se deben realizar conforme a la IETF RFC 6960. Este mecanismo de validación es complementario a la publicación de las listas de revocación de certificados (CRL).

1.3.8. Autoridad de Sellado de Tiempo

Una Autoridad de Sellado de Tiempo (TSA) es un Prestador de Servicios de Certificación que proporciona certeza sobre la existencia de determinados documentos electrónicos antes de un momento dado en el tiempo. La Autoridad de Sellado de tiempo firma la indicación temporal de dicho momento, junto con la función hash del documento al que se asocia.

ANF AC es una Autoridad de Sellado de Tiempo que gestiona un sistema informático formado por un conjunto de Servidores de Confianza, cuyo sistema horario se encuentra sincronizado con una fuente segura de tiempo.

Estos servidores reciben el nombre de Unidades de Sellado de Tiempo TSU, y tienen como función estampar sellos digitales de tiempo sobre peticiones formuladas por los usuarios de ANF AC. Permiten así determinar la existencia de un determinado objeto en el tiempo.

Los servicios de Sellado de Tiempo de ANF AC están especificados en la DPC TSA, con OID 1.3.6.1.4.1.37442.5.1.1, y cumplen con los estándares del documento IETF RFC3161, actualizado por RFC 5816, Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP) y RFC 3339 Date and Time on the Internet: Timestamps.

1.3.9. Junta Rectora de la PKI

La Junta Rectora de la PKI de ANF AC es el órgano que gestiona de forma ejecutiva la PKI, y es la responsable de la aprobación de la presente Declaración de Prácticas de Certificación y Políticas que conforman su adenda, así como de su adecuación a la normativa legal vigente, a las normas técnicas que le afectan en su materia, y su armonización con las Políticas de Certificación.

1.4. Uso del certificado

Las Políticas de Certificación correspondientes a cada tipo de certificado emitido por la ANF AC constituyen los documentos en los que se determinan los usos y limitaciones de cada certificado, y están publicadas en

https://www.anf.ec

No obstante, con carácter general, se establecen a continuación los usos permitidos y prohibidos de los certificados emitidos por ANF AC.

1.4.1. Usos apropiados

Los certificados emitidos por ANF AC y dirigidos al público en general, empresas y corporaciones privadas, están destinados a ser utilizados por los suscriptores para cualquier uso que no esté expresamente prohibido, respetando las limitaciones establecidas en el certificado o en la Política de Certificación a la que se somete, asumiendo, y por lo tanto aceptando, las limitaciones de responsabilidad declaradas por el emisor en el propio certificado, en esta DPC y PCs.

Los certificados deben emplearse para su función propia y finalidad establecida, sin que puedan emplearse para otras funciones y con otras finalidades. Del mismo modo, los certificados deben emplearse únicamente de acuerdo con la ley aplicable, especialmente teniendo en cuenta las restricciones de importación y exportación en materia de criptografía existentes en cada momento.

Las Políticas de Certificación correspondientes a cada tipo de certificado pueden determinar limitaciones y restricciones adicionales en el uso de los certificados.

Los certificados de **firma electrónica** garantizan la identidad del suscriptor y del poseedor de la clave privada de firma. Con la intervención de dispositivos seguros de creación de firma (DSCF), resultan idóneos para ofrecer soporte a la firma electrónica *"cualificada",* lo que ofrece un nivel superior de seguridad.

Los certificados electrónicos pueden también emplearse, si así se define en el tipo de certificado correspondiente, para firmar mensajes de autenticación, en particular desafíos de cliente SSL o TLS, correo electrónico seguro S/MIME, cifrado sin recuperación de claves, u otros. Esta firma digital tiene el efecto de garantizar la identidad del suscriptor del certificado de firma.

El certificado de **sello electrónico** vincula los datos de validación de un sello con una persona jurídica y confirma el nombre de esa persona. Permiten generar sellos electrónicos, que sirven como prueba de que un documento electrónico ha sido expedido por una persona jurídica, aportando certeza sobre el origen y la integridad del documento.

Los certificados electrónicos emitidos por ANF AC cumplen con las características técnicas de los perfiles descritos en la Resolución ARCOTEL-2024-0176, de fecha 16 de agosto de 2024.

Los certificados electrónicos emitidos por ANF AC se emiten en los contenedores previstos en la Resolución ARCOTEL-2024-0176, de fecha 16 de agosto de 2024:

a) Certificados en software o archivo p.12 - (PKCS #12).

b) Certificados en Dispositivos Seguros de Creación de Firma (DSCF): Dispositivos Criptográficos Seguros, Certificados Remotos o en nube (HSM) y Certificados en Tarjeta Criptográfica.

1.4.2. Usos prohibidos

Los Certificados emitidos por ANF AC y los servicios prestados en calidad de VA o TSA se utilizarán exclusivamente para la función y finalidad que tengan establecida en las correspondientes Políticas y, con arreglo a la normativa vigente, teniendo en cuenta las restricciones de importación y exportación en materia de criptografía existentes en cada momento.

Los certificados, salvo en los casos en que así lo especifique la PC, no pueden utilizarse para actuar ni como Tercero Vinculado ni como Autoridad de Certificación. Tampoco pueden utilizarse para firmar certificados de clave pública de

ningún tipo, ni listas de revocación de certificados (CRL), ni consultas de validación OCSP, ni emisión de sellos digitales de tiempo, ni para la prestación de servicios de validación o firma delegada.

Las Políticas de Certificación correspondientes a cada tipo de certificado pueden determinar limitaciones y restricciones adicionales en el uso de los certificados. No es objetivo de esta DPC la determinación de dichas limitaciones y restricciones adicionales.

Los certificados no se han diseñado ni se pueden destinar a equipos de control de situaciones peligrosas o para usos que requieren actuaciones a prueba de fallos, como el funcionamiento de instalaciones nucleares, sistemas de navegación o comunicaciones aéreas, o sistemas de control de armamento, donde un fallo pudiera directamente conllevar la muerte, lesiones personales o daños medioambientales severos, ni se autoriza su uso o reventa para dichos usos.
Las Políticas de Certificación correspondientes a cada tipo de certificado pueden determinar prohibiciones adicionales en el uso de los certificados.

1.5. Administración de la política

La propia evolución de los servicios de certificación de ANF AC conlleva que esta Declaración de Prácticas de Certificación, y las Políticas de Certificación estén sujetos a modificaciones. Se establece un sistema de versiones numeradas para la correcta diferenciación de las sucesivas ediciones que de estos documentos se produzcan.

Toda necesidad de modificación debe estar justificada desde el punto de vista técnico, ambiental, legal o comercial. Se deberán contemplar todas las implicaciones técnicas y legales de la nueva versión de especificaciones.

Se establecerá un control de modificaciones para garantizar, en todo caso, que las especificaciones resultantes cumplen con los nuevos requisitos identificados que dieron pie al cambio. En caso de que los cambios producidos puedan afectar la aceptación del servicio por parte del sujeto, suscriptor o terceros que confían, ANF AC notificará debidamente los cambios a los suscriptores y terceros que confían.

La publicación de un nuevo documento conlleva la derogación del anterior. La Junta de Gobierno de la PKI revisa cada trimestre la DPC, o cuando cualquier nueva normativa aplicable adquiera vigencia, ocurran cambios en la estructura o prestación de servicios que afectan directamente al presente documento.

1.5.1. Organización que administra el documento

La Junta Rectora de la PKI es la responsable de la administración de esta DPC y de las Políticas de Certificación de ANF AC. La fecha de publicación es la fecha de entrada en vigor.

Departamento	Junta Rectora de la PKI
Correo electrónico	msanchez@anf.ec
Dirección	Av. 12 de Octubre N24-739 y Av. Colon - Ed. Torre Boreal
Localidad	Quito
Código Postal	170143
Número de teléfono	+593 02 3826877

1.5.2. Persona de contacto

Departamento	Gerencia
Correo electrónico 1	msanchez@anf.ec
Dirección	Av. 12 de Octubre N24-739 y Av. Colon - Ed. Torre Boreal
Localidad	Quito
Código Postal	170143
Número de teléfono	+593 02 3826877

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 de una causa razonable para revocar un certificado:

- A través de la persona de contacto reseñada en esta sección 1.5.2.
- Rellenando el formulario web publicado a tal efecto.
- 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 la aplicabilidad de cada política y la conformidad con la DPC en función de los resultados y las recomendaciones recibidas de un auditor independiente (consultar la Sección 8). ANF AC también es responsable de evaluar y actuar sobre los resultados de las auditorías de cumplimiento.

1.5.4. Procedimientos de aprobación de políticas

Las modificaciones finales, así como la publicación y aspectos referidos a la notificación, son aprobados por la Junta Rectora de la PKI, tras comprobar el cumplimiento de los requisitos establecidos en este documento.

El Responsable del Departamento Jurídico y el responsable del Departamento Técnico, analizarán que los cambios propuestos en las DPC y Políticas, se encuentran alineados con las últimas versiones de las “Baseline Requeriments for the Issuance and Management of Publicly-Trusted Certificates” elaborado por el CA/B Forum, y que los mismos atienden los requerimientos que dieron motivo a la propuesta de modificación. Así mismo asumen la realización de un control anual de actualización de la DPC, Políticas de Certificación y otros documentos asociados, emitiendo el correspondiente informe de mantenimiento de versión o propuestas de cambio.

Todos los informes son sometidos a aprobación de la Junta Rectora de la PKI, la cual asume la responsabilidad de verificar su conformidad y, en su caso, emite orden de aplicación de los mismos.

1.6. Definiciones y acrónimos

1.6.1. Definiciones

Autenticación: Procedimiento de comprobación de la identidad de un suscriptor o titular de certificados.

Entidad de Certificación de Información y Servicios Relacionados Acreditada/Autoridad de Certificación (CA o AC): Es la Autoridad de Certificación, la entidad que emite certificados electrónicos.

Tercero Vinculado/Autoridad de Registro (RA o AR): Es la entidad encargada de realizar las tareas de identificación de los suscriptores, vinculada contractualmente con la Entidad de Certificación.

Autoridad de Sellado de Tiempo (TSA): Es la entidad que emite sellos de tiempo electrónicos.

Infraestructura de Clave Pública (PKI): Conjunto de personas, políticas, procedimientos y sistemas informáticos necesarios para proporcionar servicios de autenticación, cifrado, integridad y no repudio, mediante el uso de criptografía de claves públicas y privadas y de certificados electrónicos.

Clave pública y clave privada: La criptografía en la que se basa la PKI de ANF AC es la criptografía asimétrica. En ella se emplean un par de claves: lo que se cifra con una de ellas sólo se puede descifrar con la otra y viceversa. A una de esas claves se la denomina pública y está incorporada en el certificado electrónico, mientras que a la otra se la denomina privada y está bajo la custodia del titular del certificado.

Cadena de confianza: Es una lista ordenada de certificados, que contienen un certificado de un usuario final y certificados intermedios (que representan la AC subordinada), para verificar que el emisor y todos los certificados intermedios son fidedignos.

Certificado Raíz: Certificado autofirmado cuyo suscriptor es una Autoridad de Certificación (CA) perteneciente a la jerarquía de ANF AC, y que contiene los datos de verificación de firma de dicha CA, firmado con los datos de creación de firma de la misma como Entidad de Certificación de Información y Servicios Relacionados Acreditada.

Certificado Electrónico: Es el mensaje de datos que certifica la vinculación de una firma electrónica o sello electrónico con una persona natural o jurídica determinada, a través de un proceso de comprobación que confirma su identidad.

Certificado de Miembro de Empresa/ Empleado con Relación de Dependencia: Es un mensaje de datos que identifica a una persona natural o jurídica que será el signatario y su vinculación con el titular de la firma que puede ser una persona jurídica pública o privada, o con la persona natural con la que tiene relación de dependencia.

Certificado de Persona Natural: Es un mensaje de datos que identifica a la persona natural titular de la firma, mayor de edad y será responsable a título personal de todo lo que firme electrónicamente, dentro del ámbito de su actividad y límites de uso que correspondan.

Certificado de Sello Electrónico: Es un mensaje de datos que identifica a la persona jurídica pública o privada que es titular de la firma y su vinculación con el signatario, quien es responsable de su protección y custodia.

Certificado de Representante Legal: Es un mensaje de datos que identifica al representante legal o apoderado que será el signatario y su vinculación con la persona jurídica pública o privada que es el titular de la firma.

Clave de Sesión: Clave que establece para cifrar una comunicación entre dos entidades. La clave se establece de forma específica para cada comunicación, o sesión, terminando su utilidad una vez finalizada ésta.

Componente Informático (o Componente): Cualquier dispositivo software o hardware susceptible de utilizar certificados electrónicos.

Datos de activación de firma (PIN): Clave secreta que el suscriptor utiliza para activar los datos de creación de firma.

Datos de creación de firma: Es el par de clave privada asociada con el par de clave pública. Son datos únicos, clave criptográfica privada, que el suscriptor utiliza para crear la firma electrónica.

Datos de verificación de firma: Es el par de clave pública asociada con el par de clave privada. Son datos únicos, clave criptográfica pública, que se utiliza para verificar una firma electrónica.

Directorio: Repositorio de información que sigue el estándar X.500 de ITU-T.

Dispositivo: Instrumento que sirve para aplicar los datos de creación de firma.

Dispositivo seguro de creación de firma (DSCF): Dispositivos Criptográficos Seguros, Certificados Remotos o en nube (HSM) y Certificados en Tarjeta Criptográfica.

Función Hash (Hash o Huella Digital): Operación que se realiza sobre un conjunto de datos de cualquier tamaño, de forma que el resultado obtenido es otro conjunto de datos de tamaño fijo menor a los datos de entrada e independientemente del tamaño original, que tiene la propiedad de identificar unívocamente al conjunto de datos de entrada, lo cual permite garantizar la integridad de los documentos imposibilitando su falsificación.

HSM (Módulo de seguridad de Hardware): Son dispositivos de hardware, sólidos y resistentes a manipulaciones que aseguran los procesos criptográficos generando, protegiendo y administrando claves utilizadas para cifrar y descifrar datos y crear firmas y certificados digitales.

Identificación: Procedimiento de reconocimiento de la identidad de un suscriptor o titular de certificados de ANF AC.

Listas de Certificados Revocados (CRL): Lista donde figuran exclusivamente las relaciones de certificados revocados o suspendidos (no los caducados) de entidad final.

Listas de Certificados Revocados de Autoridad (ARL): Lista donde figuran exclusivamente las relaciones de certificados revocados o suspendidos (no los caducados) de CA intermedia o subordinada.

OCSP: Del inglés, (Online Certificate Status Protocol), es un método para determinar el estado de vigencia de un certificado.

RFC: Del inglés, Request For Comments, o Petición de Comentarios, es un documento cuyo contenido es una propuesta oficial para un nuevo protocolo de la red Internet que se explica con todo detalle para que en caso de ser aceptado pueda ser implementado sin ambigüedades. Se abrevia como RFC. Cada RFC tiene un título y un número.

RSA: Del inglés, Rivest-Shamir-Adleman, Es un tipo de encriptación asimétrica, que utiliza dos claves diferentes pero vinculadas. En la criptografía RSA, tanto la clave pública como la privada pueden cifrar un mensaje. Para descifrarlo se utiliza la clave opuesta a la que se utiliza para cifrar un mensaje.

Número de Serie de Certificado: Valor entero y único que está asociado unívocamente con un certificado expedido por ANF AC.

PKCS#10 (Certification Request Syntax Standard): Estándar desarrollado por RSA Labs, aceptado internacionalmente, que define la sintaxis de una petición de certificado.

Sujeto/Titular: Es la entidad o persona a la cual el certificado se le aplica y para la que se expide el certificado electrónico, que es autenticada con la clave privada y sobre la cual tiene el control.

Suscriptor: La persona física que solicita a ANF AC la emisión de un certificado electrónico, y la cual ha ratificado un Contrato de Suscripción.

Signatario: Es la persona que posee los datos de creación de la firma electrónica, quien, o en cuyo nombre, y con la debida autorización se consigna una firma electrónica.

Tercero que Confía: Persona o entidad diferente del titular que decide aceptar y confiar en un certificado emitido por ANF AC.

UIT-T: Sector de Normalización de las Telecomunicaciones de la Unión Internacional de Telecomunicaciones.

X.500: Estándar desarrollado por la UIT que define las recomendaciones del directorio. Se corresponde con el estándar ISO/IEC 9594-1: 1993. Da lugar a la serie de recomendaciones siguientes: X.501, X.509, X.511, X.518, X.519, X.520, X.521 y X.525.

X.509: Estándar desarrollado por la UIT, que define el formato electrónico básico para certificados electrónicos.

1.6.2. Acrónimos

CA/AC	Autoridad de Certificación
RA/AR	Autoridad de Registro
ARL	Authority Revocation List
AV	Autoridad de Validación
CRL	Certificate Revocation List (Lista de Revocación de Certificados)
C	Country (País).
CPD	CRL Distribution Point (Punto de Distribución de listas CRL)
CEN	Comité Européen de Normalisation
CN	Common Name (Nombre Común).
CSR	Certificate Signing Request (petición de certificado)
CWA	CEN Workshop Agreement
DN	Distinguished Name (Nombre Distintivo)
DPC	Declaración de Prácticas de Certificación
ETSI	European Telecommunications Standard Institute
HSM	Hardware Security Module (Módulo de Seguridad Hardware) cumplen el estándar ISO 15408: EAL 4 (o superior), de acuerdo con lo establecido en CEN CWA 14169
IETF	Internet Engineering Task Force (Organismo de estandarización de Internet)
IANA	Internet Assígned Numbers Authoríty. Es la entidad que supervisa la asignación global de direcciones IP, sistemas autónomos, servidores raíz de nombres de dominio DNS y otros recursos relativos a los protocolos de Internet.
LDAP	Lightweight Directory Access Protocol (Protocolo de acceso a servicios de directorio)
O	Organization
OCSP	Online Certificate Status Protocol.
OID	Object Identifier (Identificador de objeto único)
OU	Organizational Unit.
PC	Política de Certificación
PIN	Personal Identification Number (Número de identificación personal). Datos de activación de firma.
PKCS	Public Key Infrastructure Standards. Estándares de PKI desarrollados por RSA Laboratories y aceptados internacionalmente.

RSA	Rivest-Shamir-Adleman, Es un tipo de encriptación asimétrica, que utiliza dos claves diferentes pero vinculadas. En la criptografía RSA, tanto la clave pública como la privada pueden cifrar un mensaje. Para descifrarlo se utiliza la clave opuesta a la que se utiliza para cifrar un mensaje.
PKI	Public Key Infrastructure (Infraestructura de Clave Pública)
PKIX	Grupo de trabajo dentro del IETF (Internet Engineering Task Group) constituido con el objeto de desarrollar las especificaciones relacionadas con las PKI e Internet.
RFC	Request For Comments (Estándar emitido por la IETF)
UUID	Identificador universalmente único (Universally Unique Identifier)

2. RESPONSABILIDADES DE PUBLICACIÓN Y REPOSITORIO

2.1. Repositorios

Repositorio	Dirección
Certificados CA Raíz	https://crl.anf.es
Certificados CA Intermedias	
CRLs / ARLs	
Certificados Respondedor OCSP	
Estructura documental	https://www.anf.ec
Declaración de Prácticas de Certificación	
Políticas de certificación	
Documentación publicada	

2.2. Publicación de información sobre certificación

El Servicio de Publicación de ANF AC es un sistema donde se publican todos los documentos elaborados por ANF AC, relativos a sus servicios de confianza y complementarios. Así mismo se publican las certificaciones obtenidas por la entidad y las acreditaciones de que se dispone.

- Garantiza la disponibilidad de la información on line en: https://www.anf.ec
- Está disponible para cualquier interesado una versión en soporte papel completa de dicho documento.
- Emite Listas de Certificados Revocados (CRLs) y (ARL's), que se encuentran accesibles al público en general. Además, proporciona servicios de verificación en tiempo real de certificados, mediante Online Certificate Status Protocol (OCSP).

El firmante (o el Suscriptor del certificado cuando sean personas diferentes) será responsable de hacer llegar su certificado a todo aquel tercero que desee autenticar a un usuario o comprobar la validez de una firma. Generalmente, este envío se realizará de forma automática, adjuntando el certificado a todo documento firmado electrónicamente.

2.2.1. Publicación de estado de certificados emitidos

En la publicación de las Listas de Certificados Revocados, se garantiza un acceso a los usuarios y suscriptores de los certificados de forma segura y rápida, conforme a lo indicado en la sección correspondiente de esta DPC.

Además, ANF AC proporciona servicios de verificación en tiempo real de certificados en las siguientes modalidades:

- Mediante consulta Online Certificate Status Protocol (OCSP). Información en:

http://ocsp.anf.es/spain/AV

- Servicio Web disponible de forma permanente que permite consultar la situación de estado de un determinado certificado.

Salvo autorización expresa por escrito de la Junta Rectora de la PKI de ANF AC, está prohibido el uso de cualquiera de estos servicios de publicación para brindar servicios de validación a terceros o uso de la información para fines distintos que los específicamente autorizados en este documento.

2.3. Momento y frecuencia de publicación

Las CA Raíz emitirán una Lista de CAs Revocadas (ARL) como mínimo cada 90 días o extraordinariamente, cuando se produzca la revocación de un certificado de autoridad.

Cada CA Intermedia emitirá una Lista de Certificados Revocados (CRL) diariamente, y de forma extraordinaria, cada vez que se revoque un certificado.

Los certificados emitidos por la CA se publican de forma inmediatamente posterior a su emisión. ANF AC añade los certificados revocados a la lista CRL pertinente dentro del periodo de tiempo estipulado en el campo "Próxima actualización".

Las consultas OCSP se efectúan sobre estados de actualización permanente.

Cualquier modificación en las políticas y prácticas de certificación, así como cualquier cambio en las especificaciones o en las condiciones del servicio serán comunicados por ANF AC a los suscriptores y a los terceros que confían a través de la página principal de ANF AC,

https://www.anf.ec

2.4. Controles de acceso a los repositorios

La información publicada en un repositorio público es información pública. ANF AC proporciona acceso de lectura sin restricciones a estos repositorios.

El Servicio de Publicación de ANF AC cuenta con un sistema de seguridad que permite controlar de forma adecuada el acceso a la información según Clasificación de Documentos y Nivel de Seguridad de los operadores.

Este sistema impide además que personas no autorizadas puedan añadir, modificar o borrar registros de este Servicio, este proceso protege la integridad y autenticidad de la información depositada, de modo tal que:

- Únicamente las personas autorizadas puedan hacer anotaciones y modificaciones.
- Puede comprobarse la autenticidad de la información.
- Los certificados sólo estarán disponibles para consulta si el suscriptor ha prestado formalmente su consentimiento en el correspondiente contrato de suscripción.
- Puede detectarse cualquier cambio técnico que afecte a los requisitos de seguridad. ANF AC sólo permite el acceso a información clasificada a personas que están expresamente autorizadas. Se han implantado las

medidas de seguridad que permiten proteger, de forma razonable, el acceso a la información, determinando en cada consulta:

- Identidad del solicitante.
- Nivel de Seguridad acreditado

Los servidores gestionan un sistema de Log mediante el cual se realiza:

- Gestión de un registro de accesos
- Gestión de un registro de denegación de accesos

3. IDENTIFICACIÓN Y AUTENTICACIÓN

3.1. Nombres

3.1.1. Tipos de nombres

Todos los certificados contienen un nombre distinguido (Distinguished Name) X.500, en el campo Subject Name. Un "Distinguished Name" que ha sido utilizado en un certificado nunca será reasignado a otra entidad. Adicionalmente, todos los nombres de los certificados cualificados son coherentes con lo dispuesto en el apartado 7.1. Perfil de los certificados.

3.1.2. Necesidad de que los nombres sean significativos

Los campos del DN referentes al nombre y apellidos corresponden con los datos registrados legalmente del firmante, expresados exactamente en el formato que conste en la cédula de identidad o ciudadanía, el documento nacional de identidad, el pasaporte o la licencia de conducir, indistintamente.

En el caso que los datos consignados en el DN fueran ficticios o se indique expresamente su invalidez (ej. "PRUEBA" o "TEST"), se considerará al certificado sin validez legal, únicamente válido para dar cumplimiento a las obligaciones de remisión de los tipos de certificados a ARCOTEL y a MINTEL, contempladas en los numerales 20 y 21 del artículo 4 de la Resolución ARCOTEL-2024-0176, de fecha 16 de agosto de 2024, por la que se expide la "NORMA TÉCNICA PARA LA PRESTACIÓN DE LOS SERVICIOS DE INFORMACIÓN Y SERVICIOS RELACIONADOS DE LAS ENTIDADES DE CERTIFICACIÓN ACREDITADAS Y TERCEROS VINCULADOS"..

3.1.3. Anonimato o seudonimia de los suscriptores

Los certificados emitidos por ANF AC no admiten el uso de seudónimo de firmante.

3.1.4. Normas para interpretar diferentes formas de nombre

ANF AC atiende en todo caso al formato marcado por el estándar X.500 de referencia en la ISO/IEC 9594.

ANF AC garantiza que los atributos de nombres de los sujetos se introducen tal como aparecen en la documentación oficial presentada por el solicitante, en cumplimiento de la normativa aplicable. Debido a esto, es posible que, en casos puntuales, ciertos campos relacionados con los nombres de personas físicas o jurídicas superen los límites establecidos en la IETF RFC 5280. Estos casos son inevitables cuando los datos oficiales exceden dichos límites. En estos casos, se prioriza la precisión de los datos oficiales proporcionados por el solicitante, incluso si exceden los límites definidos por la norma técnica.

3.1.5. Unicidad de los nombres

El DN de los certificados debe ser único.

Dentro de una misma jerarquía no se puede volver a asignar un nombre de suscriptor que haya sido utilizado por otro suscriptor, para evitar duplicidad de nombres entre distintas personas se incorporará en su caso el identificador fiscal único a la cadena del nombre que distingue al titular del certificado.

En el Common Name (CN) se deben cumplir los requisitos de unicidad y de espacios en el nombre. En ningún caso se emiten certificados anónimos, aunque ANF AC podrá emitir certificados de pseudónimo, pero éstos no pueden ser certificados de CA o CA subordinada.

3.1.6. Reconocimiento, autenticación, y rol de marcas registradas

Los nombres distintivos son propiedad de las personas que sustentan los derechos de marca correspondiente sobre los mismos, de existir. Los suscriptores no pueden solicitar Certificados con ningún contenido que infrinja los derechos de propiedad intelectual de otra entidad. Si no se conoce esta circunstancia, ANF AC empleará el nombre propuesto por el usuario, bajo la entera responsabilidad de éste.

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

Los suscriptores de certificados no incluirán nombres en las solicitudes que puedan suponer vulneraciones de derechos de terceras partes.

Los conflictos de nombres de responsables de certificados que aparezcan identificados en los certificados con su nombre real se solucionan mediante la inclusión, en el nombre distintivo del certificado, de la cédula de identidad del responsable del certificado o de otro identificador asignado por el suscriptor.

3.2. Validación inicial de la identidad

3.2.1. Método para demostrar la posesión de la clave privada

Las claves de certificados de usuario final pueden ser generadas de diferentes maneras dependiendo de la modalidad seleccionada. La posesión de la clave privada queda demostrada en todos los casos mediante la verificación de una **Petición de Certificado (Certificate Signing Request - CSR)** conforme al estándar **RSA PKCS#10**.

Cuando las claves son generadas por el propio suscriptor, este define de manera independiente los datos de activación de firma (PIN), sin intervención de terceros. La posesión de la clave privada queda demostrada mediante la firma de la clave pública incluida en el CSR con la clave privada asociada. Esto certifica que el suscriptor tiene en su posesión el par de claves y la capacidad de utilizarlo.

En los casos en los que ANF AC genera el par de claves para el suscriptor, estas claves pueden ser almacenadas en un dispositivo criptográfico (en el caso de certificado centralizado) o entregadas al suscriptor en software en formato cifrado PKCS#12 (PFX). Cuando el certificado se entrega en software, la posesión de la clave privada se asegura internamente mediante la creación y firma del CSR en el entorno controlado de ANF AC antes de ser transmitido al suscriptor.

En todos los casos, ANF AC procesa el CSR verificando su integridad, autenticidad y conformidad con los estándares aplicables. Esto incluye validar que las claves privadas se generan utilizando algoritmos y longitudes de clave adecuados, y que la firma del CSR demuestra el control exclusivo del suscriptor sobre la clave privada. Además, este proceso permite identificar inconsistencias o errores en el contenido del CSR.

3.2.2. Autenticación de la identidad de una organización

ANF AC se basa en especificaciones y procedimientos técnicos mínimos para los niveles de seguridad de medios de identificación electrónica.

Cada Política de Certificación establece el procedimiento de autenticación de la identidad de una persona jurídica, determinando de forma general los siguientes aspectos:

- Tipos de documentos válidos para la identificación.

- Procedimiento de identificación a realizar por el Tercero Vinculado.
- Necesidad o no de identificación presencial.
- Forma de acreditar la pertenencia a una determinada organización y facultades legales suficientes de representación.

3.2.3. Autenticación de la identidad de una persona natural

ANF AC se basa en especificaciones y procedimientos técnicos mínimos para los niveles de seguridad de medios de identificación electrónica.

Cada Política de Certificación establece el procedimiento de autenticación de la identidad de una persona natural, determinando de forma general los siguientes aspectos:

- Tipos de documentos válidos para la identificación.
- Procedimiento de identificación a realizar por el Tercero Vinculado.
- Necesidad o no de identificación presencial.
- Forma de acreditar una posible representación en nombre de un tercero.

La identidad de las personas naturales se demostrará con la presentación de la cédula de identidad o ciudadanía, el documento nacional de identidad, el pasaporte o la licencia de conducir, indistintamente.

Asimismo, **se podrá emplear el método de atención virtual** para la emisión de un certificado de firma electrónica, según dispone en artículo 17 de la Resolución ARCOTEL-2024-0176, de fecha 16 de agosto de 2024, por la que se expide la "NORMA TÉCNICA PARA LA PRESTACIÓN DE LOS SERVICIOS DE INFORMACIÓN Y SERVICIOS RELACIONADOS DE LAS ENTIDADES DE CERTIFICACIÓN ACREDITADAS Y TERCEROS VINCULADOS".

Para ese caso de la atención virtual, mediante el empleo de mecanismos de autenticación biométrica u otros similares para demostrar la identidad, no será necesaria la presentación de ninguno de los documentos de identidad referidos más arriba, respecto de los ciudadanos ecuatorianos o extranjeros registrados legalmente en la DIGERCIC, contra cuyo servicio se realiza la validación de la identidad por parte de la Entidad de Certificación o del Tercero Vinculado. Ello es conforme con el art. 24 de Ley Orgánica para la optimización y eficiencia de trámites administrativos, de 16 de octubre de 2018, en concordancia con el art. 86 de la ley Orgánica de Gestión de la Identidad y Datos Civiles, de 1 de febrero de 2015.

Si el resultado de la comprobación fuera “indeterminado” (por ejemplo, para cédulas de identidad antiguas, de las que no consta la imagen digitalizada en el Registro Civil), la aplicación solicitará fotografía de la cédula de identidad o pasaporte para continuar con el proceso. La aplicación biométrica de ANF AC realiza captura de la fotografía, mediante técnicas de IA verifica que el documento de identidad es original y vigente, lee la información mediante tecnología OCR Y MRZ, y la registra en sus sistemas.

La duración del certificado se establecerá contractualmente entre el titular de la firma electrónica y la entidad certificadora de información o quien haga sus veces. En caso de que las partes no acuerden nada al respecto, el certificado de firma electrónica se emitirá con una validez de dos años a partir de su expedición. Al tratarse de certificados de firma electrónica emitidos con relación al ejercicio de cargos públicos o privados, la duración del certificado de firma electrónica podrá ser superior a los dos años, pero no podrá exceder el tiempo de duración de dicho cargo público o privado a menos que exista una de las prórrogas de funciones establecidas en las leyes.

3.2.4. Información no verificada sobre el suscriptor

No se contempla la inclusión de información no verificada en los certificados emitidos por ANF AC.

3.2.5. Validación de facultades de representación

El Responsable de Dictámenes de Emisión es el encargado de proceder a la verificación de las facultades de representación, determinando su vigencia en los registros públicos donde tengan que estar inscritas, y valorar su suficiencia.

3.2.6. Criterios para la interoperación

Ninguna estipulación.

3.3. Identificación y autenticación para solicitudes de renovación de claves

3.3.1. Identificación y autenticación para renovación de claves rutinarias

Cada Política de Certificación establece el procedimiento de autenticación de la identidad del suscriptor.

ANF AC corrobora la existencia y la validez del certificado al cual se pretende realizar la renovación de claves, y que la información utilizada para verificar la identidad y atributos del sujeto siguen siendo válidos. Por otro lado, si en la fecha de renovación de claves, han sido modificados los términos y condiciones que regían la relación entre el suscriptor/ sujeto y la CA, se deberá hacer entrega de los términos y condiciones vigentes.

3.3.2. Identificación y autenticación para renovación de claves tras revocación

No aplicable. No se autoriza la renovación de claves de certificados revocados.

3.4. Identificación y autenticación para solicitudes de revocación

ANF AC autentifica todas las solicitudes de revocación. Los solicitantes de la revocación autorizados en el apartado 4.9.2. del presente documento, disponen de los siguientes procedimientos para solicitar la revocación de su certificado:

- Cumplimentar y firmar el formulario de solicitud de revocación, disponible en formato electrónico, y papel para actos presenciales.
- Utilizar la aplicación *ANF Certificate Manager®* de ANF AC, que dispone de opción de revocación en línea con autenticación mediante certificados electrónico vigente.
- Mediante llamada telefónica al +593 02 3826877, respondiendo a las preguntas que son requeridas para garantizar identidad, y que efectúa el responsable del Departamento Jurídico de ANF AC.

4. REQUERIMIENTOS OPERATIVOS DEL CICLO DE VIDA DEL CERTIFICADO

El presente apartado establece los requisitos operativos comunes a los diferentes tipos de certificados emitidos por ANF AC. En el caso de que ANF AC realice "cross certification" con una Entidad de Certificación de Información y Servicios Relacionados Acreditada externa, ANF AC exigirá el cumplimiento de todos los requisitos definidos en la presente Declaración de Prácticas de Certificación y las Políticas de Certificado relacionadas.

La regulación específica para cada tipo de certificado deberá consultarse en la Política correspondiente.

4.1. Solicitud del certificado

4.1.1. Quién puede solicitar un certificado

Cada Política de Certificación concreta define quién puede ser titular de un certificado, quién puede aplicar para uno y los documentos acreditativos que debe suministrar.

4.1.2. Proceso de solicitud y responsabilidades

Acreditada la identidad del suscriptor ante la Autoridad de Registro o Tercero Vinculado, todo suscriptor que desee un certificado deberá:

- Cumplimentar el formulario de solicitud con toda la información en él requerida y firmarlo. No obstante, no toda la información solicitada será incluida en el certificado, y sólo es requerida para atender las obligaciones que ANF AC debe asumir para una correcta emisión y gestión de su PKI. Esta información será conservada de manera confidencial por ANF AC, de acuerdo con la normativa vigente en materia de Protección de Datos de Carácter Personal.
- Suscribir el correspondiente contrato de suscripción y adhesión a los términos y condiciones contractuales de ANF, y abonando las tasas asociadas al servicio contratado. La firma de esos documentos contractuales presupone la aceptación del certificado electrónico, y de todas las obligaciones y responsabilidades reseñadas en esta DPC y su respectiva Política de Certificación.

No será necesaria una nueva "Solicitud de Emisión" en el caso de emisiones realizadas como consecuencia de una revocación debida a fallos técnicos en la emisión y/o distribución del certificado o documentación relacionada.

Los datos que identifican al poseedor de claves en el certificado y en la solicitud son los que constan en los documentos de identificación requeridos. Esta información es registrada con exactitud, dentro de los límites de longitud derivados de los condicionantes técnicos establecidos en el contenido del certificado.

Cualquier modificación relativa a la información contenida en el certificado o de los documentos cumplimentados para tramitar la solicitud, producida con posterioridad a la emisión del certificado, debe ser comunicada a ANF AC, ya que puede conllevar una revocación del certificado.

Por otro lado, en el ámbito de certificados electrónicos de firma centralizada, las funciones de identificación y autenticación descritas en este apartado serán igualmente realizadas por un operador de una Autoridad de Registro o Tercero Vinculado.

El Tercero Vinculado asesorará a los suscriptores sobre la adecuación del tipo de certificado a las características de uso y perfil del titular. El Tercero Vinculado podrá autorizar o denegar una solicitud.

Utilizando los medios técnicos facilitados por ANF AC al Tercero Vinculado, se procede al registro en línea de la solicitud del certificado en los Servidores de Confianza de ANF AC.

En el supuesto de que no intervengan Terceros Vinculados, el suscriptor del certificado asume la responsabilidad de tramitar la documentación, autenticarla y registrarla ante ANF AC, según el procedimiento especificado en la Política de Certificación correspondiente.

ANF AC dispone de un servicio de atención al cliente. Cualquier interesado en solicitar certificados electrónicos puede recibir soporte mediante:

- Llamada telefónica +593 02 3826877
- Correo electrónico soporte@anf.ec

4.2. Procesamiento de la solicitud de certificado

4.2.1. Realización de funciones de identificación y autenticación

Los Responsables de Dictámenes de Emisión asumen la responsabilidad de valorar la suficiencia de la documentación aportada por los suscriptores, y de ordenar las comprobaciones necesarias que permitan determinar la veracidad de la información que se solicita incorporar en el certificado.

Además, ostenta la potestad de modificar cambios en la solicitud del certificado, a solicitud del AR y/o suscriptor, siempre y cuando ésta se realice previa a la emisión del certificado, y los datos hayan sido previamente contrastados por el Tercero Vinculado o el mismo Responsable de Dictámenes de Emisión.

Igualmente, están facultados para corregir los errores materiales que detecte en la solicitud, que se deriven de la constatación de los documentos aportados.

El Responsable de Dictámenes de Emisión, en base a las gestiones de comprobación realizadas, emitirá un informe de aprobación, denegación o requerimiento de ampliación documental al suscriptor.

4.2.2. Aprobación o rechazo de solicitudes

Es responsabilidad del Responsable de Dictámenes de Emisión:

- Verificar que la solicitud del certificado contiene información veraz y completa del suscriptor.
- Determinar que la solicitud se ajusta a los requisitos exigidos en la correspondiente Política, según el tipo de certificados requerido.
- Analizar los poderes de representación y otras escrituras públicas.
- Comprobar que se han suscrito todos los documentos y se han atendido todas las formalidades exigidas en esta DPC y sus políticas de certificación correspondientes.
- Verificar que la información contenida en el certificado es exacta y que no se han cometido errores mecanográficos.

- Verificar que incluye toda la información requerida, y que, en caso de incluir información no exigible, se cuenta con la autorización del suscriptor para incluirla en el certificado.
- Aplicar el correspondiente proceso criptográfico de verificación sobre el certificado de petición, a fin de comprobar la integridad de los datos contenidos en ese certificado y que el firmante está en posesión de los datos de creación de firma.

En base a toda la labor realizada, determina:

- La emisión de los certificados generando y firmando un dictamen de emisión favorable, o
- denegando la emisión, mediante dictamen desfavorable, o
- solicitando aportación de nuevos documentos acreditativos, o la firma de actas complementarias.

4.2.2.1. Denegación

Además del resultado de denegación que pueda llegar a emitir el Responsable de Dictámenes de emisión, ANF AC se reserva el derecho de denegar la emisión o renovación de certificados libremente y cuando lo estime oportuno.

Un sistema PKI se desarrolla en un marco de confianza mutua y en una relación de buena fe. Aquellas personas que mantengan o hayan mantenido directamente algún tipo de conflicto de intereses con esta entidad prestadora de servicios de certificación, o con los miembros de su Junta Rectora, no pueden tramitar solicitud alguna de emisión de certificados, ni instar a terceros a que lo realicen. Tampoco pueden realizar solicitudes de certificados personas pertenecientes o dependientes de entidades que son competencia de ANF AC.

Por otro lado, en el ámbito de certificados electrónicos de firma centralizada, se seguirá el mismo procedimiento detallado en este apartado.

4.2.3. Tiempo para procesar las solicitudes de certificado

Se establece un plazo máximo de 15 días para la tramitación de las solicitudes de certificados. ANF AC no asume responsabilidad por las demoras que puedan surgir, pero en caso de superar el plazo máximo establecido deberá informar al suscriptor de las causas que motivan la demora, quedando liberado el suscriptor para anular la petición y debiendo ANF AC retroceder cualquier cobro que haya percibido.

4.3. Emisión del certificado

La emisión de un certificado implica la aprobación final y completa de una solicitud por parte del Responsable de Dictámenes de Emisión. Según el tipo de certificado, la emisión puede efectuarse en dispositivo criptográfico o en soporte software.

4.3.1. Actuaciones de la CA durante la emisión del certificado

El Responsable de Dictámenes de Emisión emite acta de conformidad en la que queda incorporado el certificado de petición enviado por el suscriptor, así como el acta de identificación emitida por la Autoridad de Registro o Tercero Vinculado que intervino en el proceso de identificación. Notifica al suscriptor mediante correo electrónico firmado la conformidad de su solicitud.

Estos documentos son tramitados de forma automática por el servicio de emisión de certificados de ANF AC. Este servicio procede a realizar las comprobaciones de seguridad de integridad de los documentos recibidos, verifica la coherencia de los mismos y su correspondencia con la Política de Certificación a la que se someterá el certificado solicitado. En caso de conformidad, se procede a la emisión de los certificados.

Previo a la emisión del certificado, el sistema de emisión procede a la validación del formato del certificado mediante herramientas de detección de errores (linting tools).

Una vez emitido el certificado, ANF AC informa al suscriptor mediante correo electrónico, procede a activar los mecanismos informáticos necesarios para que el certificado quede inscrito en el repositorio correspondiente y esté disponible para su descarga. El suscriptor, utilizando el mismo dispositivo criptográfico de firma electrónica que empleó para generar el par de claves y el certificado de petición, podrá descargarlo e instalarlo.

ANF AC firma con su clave privada las claves públicas de los certificados que emite.

Por otro lado, en el ámbito de certificados electrónicos de firma centralizada, se seguirá el mismo procedimiento detallado en este apartado, teniendo en cuenta que el certificado una vez emitido es cargado en el dispositivo de firma centralizada en el que se generó el par de claves públicas. En ese momento el suscriptor recibe un correo electrónico informando de que el certificado ha sido emitido y está en disposición de uso en el sistema de certificados electrónicos de firma centralizada.

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

Los dispositivos criptográficos de firma electrónica de ANF AC incorporan un procedimiento que procede automáticamente a la conexión con el servidor de confianza, estableciendo una comunicación segura, que permite la descarga del certificado una vez este ha sido emitido.

Además, se remite al suscriptor un correo electrónico informando de la emisión y publicación del certificado emitido, incluido en el caso de certificados electrónicos de firma centralizada.

4.4. Aceptación del certificado

4.4.1. Conducta constitutiva de aceptación del certificado

Se establece que:

- La aceptación del certificado queda formalizada por el suscriptor con la ratificación del Contrato de Suscripción, tal y como consta en el apartado 4.1 de este documento. Además, ANF AC podrá solicitar el perfeccionamiento de la aceptación del certificado requiriendo al suscriptor que firme un Acta de Recepción y Aceptación del Certificado. Este requerimiento deberá ser atendido por el suscriptor en un plazo máximo de 15 días. Transcurrido ese plazo término sin que el suscriptor haya atendido el requerimiento, ANF AC podrá proceder a la revocación del certificado.
- En la PC correspondiente se podrá detallar o ampliar la forma en que se acepta el certificado.
- ANF AC garantiza el correcto funcionamiento de los instrumentos que suministra, que éstos funcionan de acuerdo con las características que le son exigibles. El suscriptor dispone de 7 días naturales para comprobar el certificado, el software y el dispositivo criptográfico.

- En caso de defectos de funcionamiento por causas técnicas (entre otras: mal funcionamiento del soporte del certificado, problemas de compatibilidad de programas, error técnico en el certificado, etc.) o por errores en los datos contenidos en el certificado, ANF AC revocará el certificado emitido y procederá a emitir uno nuevo en un plazo máximo de 72 horas.

Por otro lado, en el ámbito de certificados electrónicos de firma centralizada, se seguirá el mismo procedimiento detallado en este apartado.

ANF AC no es responsable de supervisar, investigar o confirmar la exactitud de la información contenida en el certificado después de su emisión. En caso de recibir información sobre la inexactitud o la no aplicabilidad actual de la información contenida en el certificado, se revocará tal como se indica en la sección 4.9.1.

4.4.2. Publicación del certificado por la CA

ANF AC, una vez emitido el certificado, procede a su publicación en los repositorios al efecto.

4.4.3. Notificación de la emisión del certificado a otras entidades

Para el caso de reconocimiento de certificados de firma electrónica emitidos en el extranjero, ANF AC notificará a la ARCOTEL los certificados emitidos por la entidad extranjera que revalide.

4.5. Par de claves y uso del certificado

4.5.1. Uso del certificado y clave privada por el suscriptor.

Las responsabilidades y limitaciones de uso del par de claves y del certificado, incluso en el ámbito de certificados electrónicos de firma centralizada, se establecen en la correspondiente PC.

De forma general, el suscriptor del certificado, en cualquier caso, deberá:

- Al recibir el certificado electrónico emitido por la CA, no hará uso del mismo hasta comprobar la correspondencia de los datos incluidos en el certificado con la información aportada por él, así como la adecuación del certificado a la solicitud que realizó. El uso del certificado electrónico por parte del suscriptor, supone su plena aceptación y conformidad.
- Garantizar el buen uso y la conservación de los soportes de los certificados.
- Emplea adecuadamente el certificado y, en concreto, cumplirá con las limitaciones de uso.
- Será diligente en la custodia de su clave privada, y mantendrá la privacidad de los datos de activación de firma con el fin de evitar usos no autorizados,
- Notificará a ANF AC y a cualquier persona que el suscriptor crea que pueda confiar en el certificado, sin retrasos injustificables:
    - La pérdida, el robo o cualquier riesgo que comprometa la clave privada.
    - La pérdida de control de los datos de activación de firma.
    - Las inexactitudes o cambios relativos a la información contenida en el certificado, instando la revocatoria del certificado cuando dicha modificación constituya causa de revocación.

- Dejará de emplear la clave privada transcurrido el periodo de validez del certificado, o cuando se haya producido revocación del mismo.
- Transferirá a los poseedores de claves las obligaciones específicas de los mismos.
- No monitorizará, manipulará o realizará actos de ingeniería inversa sobre la implantación técnica de los servicios de certificación, sin permiso previo por escrito de ANF AC.
- No comprometerá intencionadamente la seguridad de los servicios de certificación.
- No emplea las claves privadas correspondientes a las claves públicas contenidas en los certificados, con el propósito de firmar ningún certificado, como si se tratase de una Entidad de Certificación.

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

Los Terceros que Confían sólo pueden depositar su confianza en los certificados para aquello que establezca la correspondiente PC y de acuerdo con lo establecido en el campo “Key Usage” y “Extended Key Usage” del certificado.

Los Terceros que Confían han de realizar las operaciones de clave pública de manera satisfactoria para confiar en el certificado, así como asumir la responsabilidad de verificar el estado del certificado utilizando los medios que se establecen en esta DPC y en la correspondiente PC.

En cualquier caso, deberán:

- Comprobar que el certificado es apropiado para el uso que se pretende, y si carece del conocimiento suficiente para tener una comprensión plena del mismo, será su responsabilidad el asesorarse de forma independiente.
- Conocer las condiciones de utilización de los certificados conforme a lo previsto en la Declaración de Prácticas de Certificación y Políticas de Certificación a las que se somete la emisión y uso de cada tipo de certificado.
- Verificar la validez o revocación de los certificados, para lo que emplea información sobre el estado de los certificados de acuerdo con la Política de Validación de ANF AC.
- Comprobar la integridad y autenticidad de los certificados electrónicos de acuerdo con la Política de Validación de ANF AC.
- Verificar todos los certificados de la jerarquía de certificación, antes de confiar en la firma electrónica o en alguno de los certificados de la jerarquía de acuerdo con la Política de Validación de ANF AC.
- Tener presente cualquier limitación en el uso del certificado, con independencia de que se encuentre en el propio certificado, o en el contrato de verificador.
- Tener presente cualquier precaución establecida en un contrato o en otro instrumento, con independencia de su naturaleza jurídica.
- Notificar cualquier hecho o situación anómala relativa al certificado y que pueda ser considerado como causa de revocación del mismo.
- No monitorizar, manipular o realizar actos de ingeniería inversa sobre la implantación técnica de los servicios de certificación, sin permiso previo por escrito de ANF AC.
- No comprometer intencionadamente la seguridad de los servicios de certificación.

4.6. Renovación del certificado sin cambio de claves

Con una antelación suficiente, y como máximo con en los 30 días anteriores a la caducidad del certificado, se informará al usuario del certificado mediante correo electrónico, a la dirección indicada en el certificado electrónico, de que su certificado está cercano a su fecha de expiración. En ese mismo correo electrónico se indicarán los pasos a seguir para la renovación del certificado electrónico.

4.6.1. Circunstancias para la renovación del certificado

En cualquier caso, la renovación de un certificado está supeditada a:

- Que se solicite en debido tiempo y forma, siguiendo las instrucciones y normas que se establecen en la DPC de ANF AC.
- Que ANF AC o el Tercero Vinculado que intervino en su tramitación de solicitud no haya tenido conocimiento cierto de la concurrencia de ninguna causa de revocación del certificado.
- Que la solicitud de renovación de servicios de emisión se refiera al mismo tipo de certificado emitido inicialmente.
- El par de claves aún es criptográficamente confiable y no existen indicios de que la clave privada del sujeto haya sido comprometida.
- Que el certificado que se pretende renovar esté vigente en el momento de la solicitud.
- La renovación del certificado se permitirá por una sola vez. Requiriéndose con posterioridad, la formalización de nueva solicitud y proceso de identificación, por los métodos de personación ante un Tercero Vinculado o atención virtual aprobados por ANF AC.

Si las condiciones jurídicas de prestación del servicio han variado desde la emisión del certificado, ANF AC informará de este hecho al suscriptor.

4.6.2. Quién puede solicitar la renovación

Cualquier suscriptor podrá solicitar la renovación de su certificado si se cumplen las circunstancias descritas en el punto anterior. El formulario de solicitud de renovación debe estar firmado por la misma persona natural o representante legal que procesó la solicitud de certificado. En caso de representante legal, las circunstancias personales del suscriptor no deberían haber cambiado, especialmente su capacidad de representación legal.

4.6.3. Procesamiento de solicitudes de renovación

Se procederá a verificar que los datos de registro continúan siendo válidos y, si algún dato ha cambiado, éste deberá ser verificado, guardado y el suscriptor deberá estar de acuerdo con él, tal y como se especifica en la sección correspondiente de esta política.

El procedimiento aplicable a la renovación sin renovación de claves requerirá la recuperación segura de los dispositivos criptográficos donde residen las claves, antes de, en su caso, proceder al borrado seguro del dispositivo y a la nueva generación del certificado.

En caso de que los Términos y Condiciones para el Uso de los Certificados y Servicios hayan sido modificados, se entregará la nueva versión al suscriptor.

4.6.4. Notificación de nueva emisión de certificado al suscriptor

Una vez finalizado el proceso de renovación del certificado, el usuario recibirá un aviso en su correo electrónico que le indicará que ANF AC ya ha emitido el certificado renovado y que mediante la introducción del PIN de activación lo podrá descargar en el dispositivo. El usuario final ya podrá hacer uso del certificado renovado.

4.6.5. Conducta constitutiva de aceptación de la renovación

Conforme al apartado 4.4.1. del presente documento.

4.6.6. Publicación del certificado renovado por la CA

Conforme al apartado 2 del presente documento.

4.6.7. Notificación de la emisión del certificado a otras entidades

Ninguna estipulación.

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

4.7.1. Circunstancias para la renovación con cambio de claves

En el supuesto de que el motivo de la solicitud de renovación sea:

- Claves comprometidas o pérdida de fiabilidad de las mismas.

En las siguientes circunstancias:

- El certificado no está ni caducado ni revocado.
- Los datos contenidos en el certificado siguen siendo válidos y si algún dato ha cambiado, éste deberá ser verificado, guardado y el suscriptor deberá estar de acuerdo con él, tal y como se especifica en la sección correspondiente de esta política.
- Se trata de la primera renovación.

Si las condiciones jurídicas de prestación del servicio han variado desde la emisión del certificado, ANF AC o el Tercero Vinculado informarán de este hecho al suscriptor.

Se envía a la cuenta de correo electrónico que aparece en el certificado electrónico un correo donde se indican los pasos a seguir para realizar la renovación del certificado. Tras generarse el nuevo certificado y asignarle un PIN de activación, el proceso de validación y emisión es exactamente igual al de un certificado nuevo.

Por otro lado, en el ámbito de certificados electrónicos de firma centralizada, se seguirá el mismo procedimiento detallado en este apartado.

4.7.2. Quién puede solicitar la renovación con cambio de claves

Cualquier suscriptor podrá solicitar la renovación con cambio de claves de su certificado si se cumplen las circunstancias descritas en el punto anterior. Se identifica al suscriptor y se verifica que esté autorizado para requerir la renovación con cambio de claves del certificado.

4.7.3. Procesamiento de solicitudes de renovación con cambio de claves

El procedimiento aplicable a la renovación del certificado será el mismo que para la emisión de un certificado completamente nuevo. Las comprobaciones de omisión o error en la solicitud serán comprobadas por ANF AC.

En cualquier caso, la renovación de un certificado está supeditada a:

- Que se solicite en debido tiempo y forma, siguiendo las instrucciones y normas que se establecen en la DPC de ANF AC.
- Que ANF AC o el Tercero Vinculado que intervino en su tramitación de solicitud, no hayan tenido conocimiento cierto de la concurrencia de ninguna causa de revocación del certificado.
- Que la solicitud de renovación de servicios de emisión se refiera al mismo tipo de certificado emitido inicialmente.
- Que el certificado que se pretende renovar esté vigente en el momento de la solicitud.

La renovación del certificado se permitirá por una sola vez. Requiriéndose con posterioridad, la formalización de nueva solicitud y proceso de identificación, por los métodos de personación ante un Tercero Vinculado o atención virtual aprobados por ANF AC. Por otro lado, en el ámbito de certificados electrónicos de firma centralizada, se seguirá el mismo procedimiento detallado en este apartado.

En caso de que los Términos y Condiciones para el Uso de los Certificados y Servicios hayan sido modificados, se entregará la nueva versión.

4.7.4. Notificación de nueva emisión de certificado al suscriptor

Una vez finalizado el proceso de renovación del certificado, el usuario recibirá un aviso en su correo electrónico que le indicará que ANF AC ya ha emitido el certificado renovado y que mediante la introducción del PIN de activación lo podrá descargar en el dispositivo. El usuario final ya podrá hacer uso del certificado renovado.

4.7.5. Conducta constitutiva de aceptación de la renovación con cambio de claves

Conforme al apartado 4.4.1. del presente documento.

4.7.6. Publicación del certificado con cambio de claves por la CA

Conforme al apartado 2 del presente documento.

4.7.7. Notificación de la emisión del certificado a otras entidades

Ninguna estipulación.

4.8. Modificación del certificado

No aplicable.

4.9. Revocación y suspensión del certificado

4.9.1. Circunstancias para la revocación

La revocación ocasiona la pérdida de validez de un certificado antes de su caducidad. El efecto de la revocación es definitivo. Se procederá a la revocación, incluso en el ámbito de certificados electrónicos de firma centralizada, por:

1. Circunstancias que afecten a la información contenida en el certificado:
    a. Modificación de alguno de los datos contenidos en el certificado.
    b. Descubrimiento de que alguno de los datos aportados en la solicitud de certificado es incorrecto, así como la alteración o modificación de las circunstancias verificadas para la expedición del certificado.
    c. Descubrimiento de que alguno de los datos contenidos en el certificado es incorrecto.

2. Circunstancias que afecten a la seguridad de la clave o del certificado:
    a. Compromiso de la clave privada o de la infraestructura o sistemas de la Entidad de Certificación que emitió el certificado, siempre que afecte a la fiabilidad de los certificados emitidos a partir de este incidente.
    b. Infracción, por parte de la Entidad de Certificación, de los requisitos previstos en los procedimientos de gestión de certificados, establecidos en la DPC de ANF AC.
    c. Compromiso o sospecha de compromiso de la seguridad de la clave o del certificado del suscriptor o del sujeto.
    d. Acceso o utilización no autorizada, por un tercero, de la clave privada del suscriptor o del sujeto
    e. Uso irregular del certificado por el suscriptor o sujeto, o falta de diligencia en la custodia de la clave privada.
    f. La criptografía utilizada no asegura la relación entre el sujeto y la clave pública.

3. Circunstancias que afecten a la seguridad del dispositivo criptográfico:
    a. Compromiso o sospecha de compromiso de la seguridad del dispositivo.
    b. Pérdida o inutilización por daños del dispositivo criptográfico.
    c. Acceso no autorizado, por un tercero, a los datos de activación del suscriptor o del responsable de certificado.
    d. Ver apartado 4.9.1.1.

4. Circunstancias que afectan al suscriptor o responsable del certificado.
    a. Finalización de la relación entre el suscriptor y el sujeto.
    b. Modificación o extinción de la relación jurídica subyacente o causa que provocó la emisión del certificado al suscriptor o responsable del certificado.
    c. Infracción por el suscriptor del certificado de los requisitos preestablecidos para la solicitud de este.
    d. Infracción por parte del suscriptor o responsable del certificado de sus obligaciones, responsabilidad y garantías, establecidas en el instrumento jurídico correspondiente o en la Declaración de Prácticas de Certificación de la Entidad de Certificación que le emitió el certificado.
    e. Incapacidad sobrevenida o muerte del suscriptor o responsable del certificado.
    f. Extinción de la persona jurídica representada o sujeto del certificado, así como la finalización de las facultades representativas del suscriptor, cese de la autorización del suscriptor al responsable del certificado o la finalización de la relación entre suscriptor y responsable del certificado.
    g. Solicitud del suscriptor de revocación del certificado, de acuerdo con lo establecido en la sección 3.4 de esta política.

5. Otras circunstancias:
    a. La finalización del servicio de esta Entidad de Certificación y Servicios Relacionados Acreditada, de acuerdo con lo establecido en la sección 4.16 de esta política.

El instrumento jurídico que vincula a la Entidad de Certificación con el suscriptor establecerá que el suscriptor tendrá que solicitar la revocación del certificado en caso de tener conocimiento de alguna de las circunstancias indicadas anteriormente.

4.9.1.1. Pérdida de acreditación DSCF

Los dispositivos seguros de creación de firma suministrados por ANF AC a sus suscriptores, son dispositivos QSCD o SSCD publicados oficialmente por la Comisión Europea u dispositivos con nivel de seguridad FIPS 140-2 nivel 3 o superior.

En caso de que esos dispositivos pierdan el nivel de seguridad exigido, ANF AC procederá a,

- Revocar todos los certificados cuyas claves privadas fueron generadas en ese modelo de DSCF.
- Se revocará el modelo del token de su lista de dispositivos seguros.
- Se modificará el software ANF Certificate Manager® impidiendo su uso en esta aplicación.
- Se destruirán los token que se encuentran almacenados o, en caso de que el fabricante acepte su devolución, se procederá a su envío.

Dado que la revocación del certificado y del dispositivo es por causa de fuerza mayor no imputable a ANF AC, el suscriptor no recibirá compensación económica por la pérdida sobrevenida. En caso de que el fabricante del token criptográfico asuma el costo del canje, ANF AC facilitará soporte administrativo a sus suscriptores para que puedan llevarlo a cabo, pero se limitará a la sustitución del token, no a la reemisión del certificado ni a los costos de transporte.

4.9.2. Quién puede solicitar una revocación

- ANF AC
- El propio suscriptor y, en su caso, el responsable del certificado.
- El representante del suscriptor con poder suficiente.
- El Tercero Vinculado que tramitó la solicitud puede solicitar de oficio la revocación del certificado si tuviera conocimiento o sospecha del compromiso de la clave privada del titular o de cualquier otro hecho determinante que recomendará emprender dicha acción.

4.9.3. Procedimiento de solicitud de revocación

La entidad que necesite revocar un certificado, incluso en el ámbito de certificados electrónicos de firma centralizada, tiene que solicitarlo a ANF AC o, en su caso, al Tercero Vinculado ante quien tramitó la solicitud del certificado.

ANF AC dispone de un servicio 24x7 para atender revocaciones.

- **Revocación inmediata** desde las páginas:
  - https://revocarcertificado.anf.ec/ o
  - El Área personal https://myaccount.anf.ec
  - https://reportarproblema.anf.ec/key-compromise (en caso de compromiso de clave)
- **Revocación no inmediata:**
  - **En horario de oficina**, en el teléfono +593 02 3826877, enviando el formulario de solicitud de revocación firmado a soporte@anf.ec o mediante personación en sus dependencias.
  - **Fuera del horario de oficina,** mediante llamada al teléfono +593 02 3826877.

El modelo de formulario de revocación está publicado en el sitio web de ANF AC: https://www.anf.ec.
La solicitud de revocación deberá contener, como mínimo, la siguiente información:

- Fecha de solicitud de la revocación.

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

4.9.4. Período de gracia de solicitud de revocación

Las solicitudes de revocación se tramitarán de forma razonablemente inmediata cuando se tenga conocimiento de la causa de revocación y se haya autenticado al suscriptor y comprobado su capacidad de obrar. Por tanto, no existe ningún periodo de gracia asociado a este proceso durante el que se pueda anular la solicitud de revocación.

4.9.5. Plazo máximo de procesamiento la solicitud de revocación

No hay demora asociada a los métodos de revocación inmediata, pues la revocación se realiza en el momento de la recepción verificada de la solicitud de revocación.

Para las solicitudes de revocación realizadas a través de los métodos "no inmediatos", estas serán procesadas en cuanto se reciban, siguiendo el procedimiento establecido para su verificación y autenticación. La responsabilidad de dicha verificación recae en el Responsable de Dictámenes de Emisión. El tiempo máximo entre la recepción de la solicitud y la actualización del estado del certificado, haciéndolo accesible a todas las partes confiadas, será de 24 horas.

En caso de que la confirmación de la revocación no sea posible en 24 horas, ANF AC activará un procedimiento de escalado interno para priorizar la resolución del caso. Este procedimiento incluye la notificación inmediata al Responsable de Seguridad y la documentación de todas las acciones tomadas. Se registrará la causa del retraso y se implementarán medidas correctivas para evitar futuras incidencias similares. En ningún caso, una revocación sujeta a los Baseline Requirements de CA/B Forum podrá exceder el tiempo máximo permitido.

Si la solicitud de revocación requiere revocación a fecha futura, la fecha acordada será considerada como la fecha de confirmación.

Cuando un certificado es revocado, todas sus instancias son revocadas. Se informa al suscriptor, a través de la dirección de correo electrónico que consta en el certificado revocado y a la dirección física que consta en el contrato de certificación, sobre el cambio de estado del certificado revocado. ANF AC no reactivará el certificado una vez revocado.

Asimismo, en el Dispositivo Criptográfico ANF Certificate Manager se podrá consultar que el certificado ha sido revocado.

4.9.6. Requerimientos de verificación de revocación de terceros que confían

Los terceros que confían deben comprobar el estado de aquellos certificados en los que deseen confiar.

ANF AC pone a disposición de los terceros que confían un servicio de información de estado de los certificados basados en el protocolo OCSP y, acceso y descarga de las listas de certificados revocados (CRL).

4.9.7. Frecuencia de emisión de CRL y ARL

En cada certificado se especificará la dirección de la CRL que le corresponda, mediante la extensión CRLDistributionPoints.

Las CRL se emiten cuando se produzca una revocación o cada 24h como mínimo, incluso cuando no haya cambios o actualizaciones, para así asegurar la vigencia de la información publicada. En la CRL se especifica el momento programado como límite para la emisión de una nueva CRL. En su elaboración se sigue lo establecido en la RFC 5280.

ANF AC emite una ARL cada seis meses, incluso cuando no haya cambios o actualizaciones, o cuando se produzca una revocación

Por otro lado, en el ámbito de certificados electrónicos de firma centralizada, se seguirá el mismo procedimiento detallado en este apartado.

4.9.8. Periodo máximo de publicación de CRL y ARL

El cambio de estado de vigencia de un certificado debe indicarse en la CRL o, en su caso, en la ARL, en menos de sesenta minutos desde que se produzca el cambio. En base a ello, ANF publicará una nueva CRL o ARL en su repositorio en el momento de cualquier revocación.

Todas las CRL y ARL publicadas por ANF AC estarán disponibles en un histórico disponible en la web.

En cualquier caso, ANF AC emitirá una nueva CRL en su repositorio a intervalos no superiores a 7 días, y ARL a intervalos no superiores al año.

4.9.9. Disponibilidad de servicio de verificación de estado de certificado

Los terceros que confían podrán consultar los certificados publicados en el Repositorio de ANF AC, por medio de un servicio de información de estado de los certificados basado en el protocolo OCSP, o bien mediante la consulta de las Listas de Revocación CRL y ARL.

Ambos servicios están disponibles 24 horas al día, 7 días a la semana, accesibles por protocolo seguro.

4.9.10. Requisitos de verificación de estado de certificado

Los terceros que confían deberán comprobar el estado de aquellos certificados en los que deseen confiar. La verificación del estado de los certificados puede realizarse consultando la CRL y ARL más reciente emitida por ANF AC o mediante consulta OCSP.

Para el uso de las CRLs:

- Comprobar siempre la última CRL emitida. Esta puede descargarse en la dirección URL contenida en la extensión “CRL Distribution Point” del certificado.
- Comprobar adicionalmente la(s) ARL(s) pertinentes de la cadena de certificación.
- Asegurarse que la lista de revocación esté firmada por la CA que ha emitido el certificado que está comprobando.
- La CRL no incluye certificados revocados que hayan caducado.

Para el uso de OCSP:

- Se puede utilizar mediante los métodos GET o POST.

Si por cualquier circunstancia no fuera factible obtener información del estado de un certificado, el sistema que deba utilizarlo deberá desestimar su uso o, en función del riesgo, del grado de responsabilidad y de las consecuencias que se pudieran producir, utilizarlo sin garantizar su autenticidad en los términos y estándares que se recogen en esta política.

4.9.11. Otras formas de información de revocación de certificados disponibles

Además del servicio de consulta en línea mediante protocolo OCSP (Online Certificate Status Protocol), y de consulta de las Listas de Revocación (CRL) / (ARL), ANF AC pone a disposición del público en general:

- **Servicio Web**

  Permite la comprobación del estado de vigencia mediante consulta en la web de ANF AC: https://crl.anf.es/

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

En caso de compromiso de la clave privada de un certificado de usuario final, cualquier persona puede notificar la circunstancia a ANF AC para que se proceda a la revocación del certificado. Puede notificarse desde https://www.anf.ec
apartado "*Reportar clave comprometida*" aportando un CSR que se cree con un Common Name "*Evidencia de compromiso de clave para ANF AC*" (o similar) o la misma clave privada. ANF AC comenzará la investigación dentro de las 24h posteriores a su recepción, y decidirá si se justifica la revocación u otra acción apropiada en base a la normativa aplicable vigente.

En caso de compromiso de la clave privada de la CA, será notificado el compromiso de la clave a todos los participantes de esa Jerarquía, en especial a:

- la Junta Rectora de la PKI;
- todos los Terceros Vinculados;
- todos los titulares de certificados emitidos por esa CA;
- y terceros que confían de los que se tenga conocimiento.

Además, se publicará en la Web de ANF AC, y se procederá a su inmediata revocación.

La CA Raíz publicará el certificado revocado en la ARL (Lista de Revocación de Autoridades de Certificación). Después de resolver los factores que indujeron a la revocación, ANF AC puede:

- Generar un nuevo certificado para la CA emisora.
- Asegurar que todos los nuevos certificados y CRL emitidos por la CA son firmados utilizando la nueva clave.
- La CA emisora podrá emitir certificados a todos los suscriptores afectados que así se lo requieran.

Por otro lado, en el ámbito de certificados electrónicos de firma centralizada, ANF AC como responsable de la custodia del certificado, deberá notificar esta circunstancia al suscriptor del certificado y responsabilizarse de su revocación. Además, deberá:

- Notificar a la Junta Rectora de la PKI y a los miembros del Comité de Seguridad, informe detallado de la incidencia ocurrida, y
- emitir un nuevo certificado gratuito al suscriptor que se lo requiera.

4.9.13. Circunstancias para la suspensión

No aplicable. ANF AC no autoriza la suspensión temporal de certificados.

4.9.14. Quién puede solicitar una suspensión

No aplicable.

4.9.15. Proceso de solicitud de suspensión

No aplicable.

4.9.16. Límites en el periodo de suspensión

No aplicable.

4.10. Servicios para comprobación de estado del certificado

4.10.1. Características operativas

ANF AC ofrece el servicio gratuito de publicación en Web de Listas de Certificados Revocados (CRL) sin restricciones de acceso y el libre acceso a validación de certificados en línea por medio del protocolo OCSP.

Las respuestas de OCSP de ANF AC se ajustan a RFC6960. Las respuestas de OCSP están firmadas por un Respondedor de OCSP cuyo Certificado está firmado por la CA que emitió el certificado cuyo estado de revocación se está verificando. El certificado de firma de OCSP contiene una extensión de tipo id-pkix-ocsp-nocheck, según se define en la RFC6960.

ANF AC admite consultas OCSP mediante el método GET para certificados emitidos de acuerdo con los Baseline Requirements.

Para certificados de usuario final, las respuestas OCPS emitidas por ANF AC tienen un intervalo de validez[1] mayor o igual a 8 horas, y menor o igual a 10 días.

- Para las respuestas OCSP con intervalos de validez mayores o iguales a 16 horas, ANF AC actualizará la información proporcionada a través de un OCSP al menos 8 horas antes del nextUpdate, y no más tarde de 4 días después de thisUpdate.
- Para las respuestas OCSP con intervalos de validez de menos de 16 horas, ANF AC actualizará la información proporcionada a través de un OCSP antes de la mitad del período de validez antes del nextUpdate.

En el caso de certificados de CA intermedia, ANF AC actualiza la información proporcionada a través de un OCSP al menos cada 12 meses; y dentro de las 24 horas posteriores a la revocación de un certificado de CA intermedia.

El número de serie de un certificado permanece en la CRL hasta que el certificado caduque. No obstante, la información sobre el estado de revocación del certificado, incluida la confirmación de si ha sido revocado, permanece disponible a través del servicio OCSP incluso después de su caducidad. Esto garantiza la posibilidad de verificar el estado del certificado más allá de su período de vigencia.

[1] *El intervalo de validez de una respuesta OCSP es la diferencia de tiempo entre el campo thisUpdate y nextUpdate, inclusive. Para calcular las diferencias, una diferencia de 3600 segundos será igual a una hora y una diferencia de 86 400 segundos será igual a un día.*

4.10.2. Disponibilidad del servicio

Los servicios de comprobación del estado del certificado están disponibles 24x7. La utilización del servicio OCSP es público y gratuito.

ANF AC opera y mantiene sus CRL y OCSP con recursos suficientes para proporcionar un tiempo de respuesta de cinco segundos o menos en condiciones normales de operación.

En caso de fallo del sistema, o cualquier otro factor que no esté bajo el control de la CA como se estipula en el apartado 9.16.5. del presente documento, ANF AC realizará los mayores esfuerzos para asegurar que este servicio de información no se encuentre indisponible durante más tiempo que el periodo máximo de 24 horas.

Si la ANF AC cesa su actividad, sus claves caducan o se ven comprometidas, se emitirá una última Lista de Revocación de Certificados (CRL, conocida como *lastCRL*[2]). Esta última CRL permanecerá íntegra y accesible para consulta, garantizando la disponibilidad del servicio de verificación del estado de los certificados durante un período mínimo de 15 años a partir de su publicación.

La disponibilidad de la información sobre el estado de revocación de los Certificados, en caso de que ANF AC cese su actividad como Prestador de Servicios de Confianza, estará garantizada mediante la transferencia de toda la información relacionada con los Certificados, y en particular los datos sobre su estado de revocación, a ARCOTEL, a otra Entidad de Certificación, siguiendo el procedimiento legal vigente al momento del cese.

4.10.3. Características opcionales

Ninguna estipulación.

4.11. Fin de suscripción

El certificado cuando acaba su periodo de vigencia o bien cuando ha sido revocado deja de ser válido para su uso. En cada Política de Certificación especifica la caducidad de los diferentes certificados.

4.12. Custodia y recuperación de claves

4.12.1. Política y prácticas de custodia y recuperación de claves.

En el caso de certificados electrónicos almacenados en dispositivos personales, token software criptográficos o token HSM, ANF AC no genera las claves de sus suscriptores. En el ámbito de certificados electrónicos de firma centralizada, ANF AC realizará una copia de seguridad de los datos de creación de firma, siempre que la seguridad de los datos duplicados sea del mismo nivel que la de los datos originales, y que el número de datos duplicados no supere el mínimo necesario para garantizar la continuidad del servicio. No se duplicarán los datos de creación de firma para ninguna otra finalidad.

4.12.2. Política y prácticas de encapsulación y recuperación de claves de sesión

Ninguna estipulación.

---

[2] *Una lastCRL es una Lista de Revocación de Certificados (CRL) en la que el campo nextUpdate se establece con el valor 99991231235959Z, conforme a lo indicado en la IETF RFC 5280, lo que implica que no se emitirán CRLs posteriores.*

5. INSTALACIONES, GESTIÓN Y CONTROLES OPERATIVOS

5.1. Controles físicos

Se mantienen controles en todos aquellos lugares en los que ANF AC presta servicios.

5.1.1. Ubicación del sitio y construcción

Los inmuebles donde se encuentra ubicada la infraestructura de ANF AC disponen de medidas de seguridad de control de acceso, de forma que no se permite la entrada salvo que las personas hayan sido debidamente autorizadas.

Las instalaciones en las que se procesa información cumplen los siguientes requisitos físicos:

a. El edificio que contiene las unidades de procesamiento de información es físicamente sólido, los muros externos del emplazamiento son de construcción sólida y únicamente se permite el acceso a personas debidamente autorizadas.

b. Todas las puertas y ventanas están cerradas y protegidas contra accesos no autorizados.

c. La generación de las claves y emisión de los certificados de la CA se realiza en un Centro de Procesamiento de Datos con medidas de protección adecuadas según los requerimientos establecidos en las políticas de SGSI de ANF AC. Este inmueble cuenta con una estructura física que garantiza plenamente que el lugar se encuentra libre de radiación electromagnética, dispone de servicio de seguridad 24x7x365, y múltiples barreras que impiden el acceso a personas no autorizadas.

d. Los equipos informáticos que prestan servicio al público (principal y espejos) están instalados en Centro de Procesamiento de Datos perteneciente a compañía operadora de comunicaciones nacional, con instalaciones adecuadas a ese fin, y que cuenta con infraestructura adecuada para garantizar un servicio estable, seguro y continuo.

e. El edificio donde se encuentra instalada la infraestructura central de ANF AC es un recinto físicamente seguro, dotado de hasta seis niveles de seguridad para poder llegar a acceder a las máquinas y aplicaciones críticas.

   Los sistemas están físicamente separados de otros existentes en el lugar, de forma que sólo personal autorizado de ANF AC puede acceder a ellos, garantizando así la independencia de otros equipos y sistemas de terceros alojados en el lugar.

f. Entre las medidas de protección que poseen estas instalaciones, cabe reseñar que:

   - Las instalaciones cuentan con servicio de vigilancia independiente a ANF AC de 24 horas y control por circuito de televisión cerrado permanente. Las cámaras no tienen posibilidad de efectuar visionado de las operaciones que se realizan en los servidores de ANF AC, a fin de evitar cualquier riesgo de visualización de los PIN de activación al ser introducidos u otros datos confidenciales.

   - Su situación se encuentra alejada de sótanos, para prevenir posibles inundaciones.

   - El edificio es un inmueble moderno, construido al efecto y de uso exclusivo del operador. Ubicado en zona empresarial de reconocido prestigio, de fácil y rápido acceso, en caso de necesidad, por parte de los servicios de Orden Público y Bomberos.

- El edificio se encuentra ubicado en zona de baja actividad sísmica y sin antecedentes de catástrofes naturales.
- El edificio se encuentra ubicado en zona de bajos niveles de delincuencia.
- Ni el edificio, ni la zona en donde se encuentra, están considerados objetivos terroristas.
- Las instalaciones no poseen ventanas al exterior.
- Las instalaciones se encuentran protegidas constantemente por personal perteneciente a la empresa de seguridad autorizada.

  Este personal tiene relación detallada y actualizada de las personas que ANF AC autoriza a acceder al núcleo central (donde se encuentran los equipos informáticos de ANF AC), y confeccionan un registro del día y hora de entrada y salida, identidad y firma de la persona que accede y de cada una de las personas que la acompañan, entregando tarjeta de acceso personal. En ningún caso permite la extracción de equipos infomáticos sin autorización expresa.
- El acceso al núcleo central se realiza superando distintos controles. El personal que accede se encuentra en todo momento acompañado por personal responsable de la administración del centro de datos y cualquier labor que se realiza sobre los equipos informáticos de ANF AC se realiza en presencia constante de un técnico perteneciente al personal responsable de la administración del centro de datos.
- Todas las instalaciones cuentan con sistemas de energía y aire acondicionado redundantes, que cumplen con las normas industriales, a fin de crear un entorno operativo adecuado.
- Todas las instalaciones cuentan con mecanismos de prevención destinados a reducir el efecto del contacto con el agua.
- Todas las instalaciones cuentan con mecanismos de prevención y protección contra incendios. Dichos mecanismos cumplen con las normas industriales.
- Todo el cableado está protegido contra daños o interceptación electromagnética o interceptación de la transmisión tanto de datos como de telefonía.
- Las mamparas que protegen las zonas centrales del núcleo son transparentes y cuentan con iluminación permanente, todo ello con el fin de posibilitar la observación desde cámaras de vigilancia o desde pasillos o incluso zona de oficinas administrativas, impidiendo así actividades ilícitas en el interior del Centro de Procesamiento de Datos (Datacenter).

5.1.2. Acceso físico

- **Perímetro de seguridad física:**

  Además de las medidas reseñadas anteriormente, se han implementado sistemas de control de acceso personalizado, que registran el paso de las personas por cada zona. Asimismo, se ha establecido que el personal visitante tiene que estar permanentemente tutelado por un responsable del centro de datos.

- **Controles físicos de entrada:**

  Se dispone de un exhaustivo sistema de control físico de personas a la entrada y a la salida que conforma diversos anillos de seguridad, y que es regularmente revisado.

Se combinan diversos sistemas de seguridad, humanos y técnicos, en la realización de los controles físicos de entrada:

- Acceso a la entrada identificándose mediante documento legal de identidad ante el servicio de seguridad, monitoreando y registrando persona, hora de llegada, salida, autorización que ostenta y dotando de un número de identificación personal.
- Uso del número personal para su identificación ante los dispositivos de seguridad, comprobando autorización y registrando accesos.
- No se permite la entrada salvo que las personas hayan sido debidamente autorizadas por algún miembro de la Junta de la PKI, del Responsable de Seguridad, del Director Técnico, o del Responsable Legal.

- **Introducción o extracción de equipos:**
  - Se requiere autorización expresa del Responsable de Seguridad para la realización de estas operaciones, llevando un inventario del material existente y de las entradas y salidas que se han producido.
  - ANF AC implementa controles para evitar pérdidas, daños o compromiso de los activos, e interrupción de la actividad, de acuerdo con un Plan de Continuidad de Negocio y Recuperación de Desastres
- **Seguridad contra intrusos**
  - Las instalaciones donde se encuentran los servidores de certificación, y donde se realiza el proceso de emisión de certificados de entidad final y CA, cuentan con puertas contra incendios y sistemas de detección de intrusos, que están instalados y son probados con regularidad para cubrir todas las puertas exteriores del edificio.
  - Las instalaciones que alojan los servidores están permanentemente operativas 24 horas los 365 días del año.
  - Asimismo, las instalaciones donde se realizan los procesos de generación de claves de la CA, y emisión de certificados, disponen de medidas de seguridad y alarmas para evitar cualquier tipo de allanamiento.

5.1.3. Alimentación eléctrica y aire acondicionado

Las salas donde se ubican los equipos que componen los sistemas de certificación de ANF AC disponen de suministro de electricidad y aire acondicionado suficiente para crear un entorno operativo fiable. La instalación está protegida contra caídas de corriente o cualquier anomalía en el suministro eléctrico mediante una línea auxiliar independiente de la fuente eléctrica principal.

Se han instalado mecanismos que mantienen controlados el calor y la humedad a niveles acordes con los equipos que se encuentran instalados en el lugar.

Aquellos sistemas que lo requieren disponen de unidades de alimentación ininterrumpida y grupo electrógeno.

Las instalaciones donde se encuentran los servidores de certificación, y donde se realiza el proceso de emisión de certificados de entidad final y CA, cuentan con las siguientes prestaciones:

- Los servidores que prestan servicios de certificación cuentan con sistema de protección contra fallas de energía y otras anomalías eléctricas, y todo el sistema de cableado está protegido contra interceptación y daño.
- Los equipos para la emisión de certificados están permanentemente desconectados del suministro eléctrico, y para su activación se utilizan exclusivamente fuentes de alimentación autónomas y libres de toda posible anomalía.

5.1.4. Exposiciones al agua

Se han tomado las medidas adecuadas para prevenir la exposición al agua de los equipos y el cableado.

5.1.5. Prevención y protección contra incendios

Las salas disponen de los medios adecuados -detectores- para la protección de su contenido contra incendios. El cableado se encuentra en falso suelo o falso techo y se dispone de los medios adecuados -detectores en suelo y techo para la protección del mismo contra incendios.

5.1.6. Sistema de almacenamiento de datos

ANF AC ha establecido los procedimientos necesarios para disponer de copias de respaldo de toda la información de su infraestructura productiva.

Se han establecido planes de copia de respaldo de toda la información sensible y de aquella considerada como necesaria para la persistencia de su actividad.

ANF AC almacena y custodia todos los certificados y la información relativa a los mismos durante toda la vigencia de la acreditación. Una vez concluida la acreditación se dará a esa información el tratamiento que disponga en Ordenamiento vigente.

5.1.7. Eliminación de residuos

ANF AC ha elaborado una política que garantiza la destrucción de cualquier material que pudiera contener información, así como una política de gestión de los soportes portables.

Los soportes que contienen información confidencial se destruyen de tal manera que la información es irrecuperable con posterioridad a su desecho.

5.1.8. Copia de seguridad fuera de las instalaciones

El almacenamiento de las copias de seguridad fuera de las instalaciones, se realiza en bunker bancario. Cada dispositivo de almacenamiento cuenta con un identificador único, descripción, modelo y marca.

ANF AC ha contratado en una entidad bancaria una caja de seguridad en la que se depositan copias de los dispositivos que permiten la regeneración del sistema en caso de siniestro.

El acceso a la Caja de Seguridad está restringido a personal expresamente autorizado de ANF AC, los cuales tienen en su poder una de las llaves que permite la apertura de la Caja de Seguridad.

Entre las medidas de protección que poseen estas instalaciones bancarias, reseñar que:

- Las instalaciones cuentan con servicio de vigilancia de 24 horas y control por circuito de televisión interno permanente.
- La arquitectura y blindaje del edificio corresponden al diseño comúnmente empleado en establecimientos denominados “búnker bancario”.

- Las instalaciones se encuentran protegidas constantemente por personal perteneciente a empresa de seguridad autorizada.
- El personal al que la entidad bancaria tiene encomendada la administración de los accesos confecciona un registro del día y hora de entrada y salida, identidad y firma de la persona que accede.
- El acceso al núcleo central se realiza superando distintos controles. El personal que accede se encuentra en todo momento acompañado por el personal responsable de la administración del búnker bancario y la operación de apertura de la caja bancaria se realiza mediante doble llave: una en poder del personal de ANF AC y otra en poder del personal de la entidad bancaria.
- Todas las instalaciones cuentan con sistemas de energía y aire acondicionado, que cumplen con las normas al efecto.
- Todas las instalaciones cuentan con mecanismos de prevención y protección contra incendios. Dichos mecanismos cumplen con las normas industriales.
- Para acceder a la Caja de Seguridad se requiere la presencia de al menos dos de los operadores autorizados, y el uso de la llave maestra del supervisor del bunker.

5.2. Controles de procedimiento

ANF AC administra el acceso a los sistemas de tratamiento de la información, a operadores debidamente autorizados, administradores y auditores del sistema. Estos controles incluyen la gestión de las cuentas de usuario, la modificación o eliminación oportuna del acceso.

5.2.1. Roles de confianza

ANF AC cuenta con una política de control de acceso a la información. Las funciones del sistema de aplicación están restringidas por su Sistema de Gestión de Seguridad de la Información (SGSI).

- El SGSI define suficientes controles de seguridad y establece separación de Roles, identifica responsabilidades, realiza una separación entre la administración de seguridad y las funciones de operación. En particular, establece normas que restringen y controlan el uso de los programas de utilidad del sistema.
- Todo el personal de ANF AC es identificado y autenticado antes de usar aplicaciones críticas relacionadas con el servicio.
- Los operadores del sistema son responsables de sus actividades, por ejemplo, retención de registros de eventos. Además, ANF AC cuenta con una política de personal que contempla medidas y procedimientos disciplinarios.
- El Comité de Seguridad contempla y supervisa la adopción de medidas apropiadas en el tratamiento de riesgos, teniendo en cuenta desde comerciales a técnicos, garantizando que el nivel de seguridad de la información es proporcional al nivel de riesgo.

Se distinguen los siguientes responsables para el control y gestión del sistema:

Responsables de emisión de certificados
Son un mínimo de tres los operadores que cuentan con la capacidad para acceder y activar los dispositivos de emisión de certificados de ANF AC. Para activar las claves, es necesaria la presencia de al menos dos personas de acuerdo con el requisito control dual.
Directores de área
Son las personas que asumen la dirección de cada sección de ANF AC. Bajo su control y supervisión, se encuentra el personal adscrito a la misma. Es su responsabilidad: • Recibir y dar curso a las denuncias por infracciones que puedan afectar a su personal, proponiendo las medidas disciplinarias correspondientes. • Efectuar un control permanente de la adecuación de los recursos materiales y humanos que cuenta su Departamento, con el fin de atender las necesidades de servicio que tiene encomendadas. • El personal directivo deberá poseer experiencia o capacitación en relación al servicio de confianza que se proporcione.
Administradores de sistemas
Es personal adscrito al área de Informática y Telecomunicaciones. Ninguno de ellos está implicado en tareas de auditoría interna. Es su responsabilidad: • La instalación y configuración de sistemas operativos, de productos de software y del mantenimiento y actualización de los productos y programas instalados. Cuentan con capacidad para instalar, configurar y mantener los sistemas confiables de TSP, pero sin acceso a los datos. • Activar los servicios de CRL, OCSP y Timestamping mediante certificados específicos. • Establecer y documentar los procedimientos de monitorización de los sistemas y de los servicios que prestan, así como el control de las tareas realizadas por los Operadores de la Autoridad de Certificación. • El diseño de las arquitecturas de programación, el control y supervisión de los desarrollos encomendados y la correcta documentación de las aplicaciones. • Supervisar la correcta ejecución de la Política de Copias, en particular, de mantener la información suficiente como para poder restaurar cualquiera de los sistemas en el menor tiempo posible, velar para que se lleven a cabo las copias de seguridad locales y el traslado de las mismas de acuerdo con lo establecido en el Plan de Seguridad. • Mantener el inventario de servidores y resto de componentes de los sistemas de certificación de ANF AC. • La gestión de los servicios de “router” y de reglas de firewall, gestión y mantenimiento de los sistemas de detección de intrusiones, y otras tareas relacionadas. • La instalación o eliminación de hardware criptográfico de la CA. • El mantenimiento o reparación de equipos criptográficos de la CA (incluida la instalación de nuevo hardware, firmware o software), y la eliminación de los desechables. • Los operadores de la PKI que intervienen en la gestión del día a día de los sistemas, están autorizados a realizar copias de seguridad y las recuperaciones para el correcto funcionamiento de la infraestructura de la CA.

Operadores de la Autoridad de Certificación
• Adscritos al área administrativa. • Realizan labores administrativas que no requieren acceso físico a los Servidores de Certificación. • Efectúan labores administrativas tradicionales: archivo, introducción de datos, recepción y expedición de correo, atención de visitas y llamadas telefónicas, etc. • Esencialmente colaboran en todas aquellas funciones que le son requeridas por los directores de área, bajo cuyo criterio se organiza su trabajo y delegación de responsabilidades. • Deben de haber efectuado una formación específica en materia de protección de datos y seguridad informática, superando los test correspondientes. Se exige una experiencia mínima de un año en funciones administrativas.
Responsables de selección y formación
• Adscrito al área jurídica. • Se encarga de mantener actualizados los planes de formación del personal que presta sus servicios en ANF AC. • Supervisa la realización de la formación y grado de confianza por parte del personal y lleva a cabo los test necesarios para poder evaluar el nivel adecuado de conocimientos asimilados. • Gestiona la selección de nuevo personal, controlando la obtención de referencias y del cumplimiento de los niveles establecidos. • Se exige una experiencia mínima de un año en este tipo de funciones.
Responsable de seguridad
De acuerdo con lo definido en la Política de SGSI, en especial: • Responsabilidad general de administrar la implementación de las prácticas de seguridad. • Controla la formalización de los convenios entre el personal y ANF AC. • Comunica las medidas disciplinarias acordadas, supervisando su cumplimiento. • Debe cumplir y hacer cumplir las políticas de seguridad de ANF AC, y debe encargarse de cualquier aspecto relativo a la seguridad de la PKI, desde seguridad física hasta la seguridad de las aplicaciones, pasando por seguridad de la red. • Es el encargado de gestionar los sistemas de protección perimetral y en concreto de verificar la correcta gestión de las reglas de los firewalls. • Es el encargado de comprobar la correcta instalación, configuración y gestión de los sistemas de detección de intrusiones (IDS) y de las herramientas asociadas a éstos. • Es el responsable de resolver o hacer que se resuelvan las incidencias de seguridad producidas, de eliminar vulnerabilidades detectadas, y otras tareas relacionadas. • Es el responsable de la gestión y control de los sistemas de seguridad física, y de los movimientos de material fuera de las instalaciones de la CA. • Debe encargarse de efectuar la selección y determinar la contratación de terceros especialistas que puedan colaborar en la mejora de la seguridad de ANF AC. • Se exige una experiencia mínima de un año en estas funciones. • Deberá tener familiaridad con los procedimientos de seguridad, seguridad de la información y evaluación del riesgo.

Auditores
• Adscritos al área jurídica y al área de informática y telecomunicaciones. • Realizan funciones de Auditoría Interna. • Asumen la responsabilidad de realizar la Auditoría Interna de acuerdo con las Normas y Criterios de Auditoría de los Servicios de Certificación (ANF AC). • Cuentan con la capacidad de acceder a los (registros y archivos) del sistema. • Se exige una permanencia mínima de un año en el área relacionada.
Responsable de la elaboración de dictámenes de emisión y revocación de certificados
Es el responsable de validar las peticiones, y en dictaminar sobre la emisión de un certificado.
Responsable de documentación
• Adscrito al área administrativa. • Controla que el repositorio de documentación electrónica de ANF AC y los archivos de documentación en papel están actualizados. • Supervisa que se lleve a cabo la actualización de documentos cuando sea preciso. • Es el único habilitado para almacenar, borrar o modificar documentos en el repositorio de documentación de ANF AC.

5.2.2. Número de personas requeridas por tarea

ANF AC garantiza al menos dos personas para realizar las tareas que requieren control multipersona y que se detallan a continuación:

- La generación de la clave de las CA raíz e intermedia.
- La recuperación y copia de seguridad de la clave privada de las CA raíz e intermedia.
- Ceremonia de emisión de certificados de las CA raíz e intermedia.
- Control sobre cualquier actividad realizada sobre los recursos hardware y software que dan soporte a las CA raíz.

5.2.3. Identificación y autenticación de cada rol

El personal de TSP deberá ser formalmente nombrado para las funciones de confianza por la alta dirección responsable de la seguridad

ANF AC cuenta con una Política de Roles que determina los privilegios mínimos que debe de tener un responsable de área para otorgar y configurar privilegios de acceso.

5.2.4. Roles que requieren separación de tareas

Las tareas de Auditor son incompatibles en el tiempo con las tareas de los otros roles de confianza. Estas funciones estarán subordinadas y reportará a la Junta Rectora de la PKI.

Las personas implicadas en Administración de Sistemas no podrán ejercer ninguna actividad en las tareas de Auditoría o Certificación.

5.3. Controles de Personal

5.3.1. Requisitos de calificación, experiencia y acreditaciones

De acuerdo con lo establecido en el Plan de Seguridad Administrativa.

La Política de Seguridad Administrativa y la DPC establecen la configuración del personal necesario para llevar a cabo de forma adecuada las operaciones de la AC. Siempre se sigue el principio de necesidad cierta para otorgar una autorización de acceso en un transaccional de la AC. Los responsables de área son las personas encargadas de establecer en cada momento el número de operadores, la cualificación que deben poseer según trabajo a realizar, y de seleccionar la identidad de los mismos.

En operaciones especialmente sensibles, siempre se contará con personal redundante. Se trata de personal que ha recibido la capacitación necesaria para atender este tipo de operaciones, y cuyo número siempre es superior al realmente necesario para afrontar cualquier incidencia.

ANF AC cuenta con una Política de Personal que supervisa que los operadores de la PKI, estén libres de conflictos e intereses personales, que puedan perjudicar a la imparcialidad en las funciones que les son encomendadas. Antes de la participación de cualquier persona en el Proceso de gestión de certificados, ya sea como empleado, agente o subcontratado de la CA, ANF AC verifica la identidad y confiabilidad de dicha persona.

5.3.2. Verificación de antecedentes

De acuerdo con lo establecido en el Plan de Seguridad Administrativa, cabe reseñar que los contratistas que realizan funciones de confianza están sujetos al mismo plan.

El personal no tendrá acceso a funciones de confianza, hasta que se completen los controles definidos en la Política de Personal.

5.3.3. Requerimientos de formación

ANF AC desarrolla periódicamente, al menos cada doce meses, ejercicios de capacitación dirigidos al personal que interviene en los sistemas de la CA. Esta formación puede contemplar una combinación de capacitación, credenciales o experiencia en el desarrollo de las funciones que le son encomendadas. Se presta máxima atención a formación sobre los siguientes aspectos:

- Control de acceso.
- Gestión de soportes.
- Registro de incidencias.
- Registro de usuarios.
- Identificación y autenticación.
- Copias de respaldo y recuperación.

- Análisis de ficheros, datos y sistemas informáticos.
- Sistema de seguridad de acceso a terminales de computación.
- Seguridad administrativa. Plan de Seguridad.

Se incluyen en la formación los siguientes aspectos:

- Entrega de una copia de la Declaración de Prácticas de Certificación.
- Concienciación sobre la seguridad física, lógica y técnica.
- Operación del software y hardware para cada papel específico.
- Procedimientos de seguridad para cada rol específico.
- Procedimientos de operación y administración para cada rol específico.
- Procedimientos para la recuperación de la operación de la PKI en caso de desastres.
- Seguridad y protección de datos personales.

ANF AC mantiene las evidencias de dicha capacitación y garantiza que el personal encargado mantenga un nivel de habilidad que les permita desempeñar tales deberes de manera satisfactoria. ANF AC mantiene evidencias de que los RDE poseen las habilidades requeridas para una tarea antes de permitir que realicen sus tareas. ANF AC requiere que todos los RDE aprueben un examen sobre los requisitos de verificación de solicitudes aplicables a cada tipo de certificado.

5.3.4. Frecuencia de formación continua y requisitos

Según el Plan de Formación Anual de ANF Autoridad de Certificación. Todo el personal en roles de confianza deberá mantener niveles de habilidad consistentes con los programas de formación de ANF AC.

5.3.5. Frecuencia y secuencia de rotación de trabajos

Ninguna estipulación.

5.3.6. Sanciones por acciones no autorizadas

El personal está sometido a un proceso de régimen disciplinario previamente advertido y conocido por todos los operarios de la organización. La operativa del procedimiento seguido queda documentada en la Normativa Interna, que incluye una política de sanciones.

La realización de operaciones no autorizadas, incumplimiento de políticas o procedimientos está sujeta a medidas disciplinarias. La sanción puede llegar al despido, con independencia de lo establecido en el marco legislativo que puede conllevar paralelamente la denuncia ante la Autoridad Judicial.

5.3.7. Requisitos de contratación de terceros

Todo el personal con acceso a los servicios de certificación de ANF AC firma un acuerdo de confidencialidad como parte de los términos y condiciones de su incorporación. ANF AC verifica que dicho personal cumpla con los requisitos de formación de la sección 5.3.3. y los requisitos de retención de documentos y registro de eventos de la sección 5.4.1.

Este acuerdo contempla información sobre la labor de control y fiscalización que los responsables de seguridad de ANF AC realizan permanentemente sobre el personal, el software y el hardware.

El fin de esta actividad es garantizar el más alto grado de seguridad de los servicios que esta CA presta, y de los bienes que tiene la obligación de proteger.

5.3.8. Documentación suministrada al personal

Se facilitará el acceso a la normativa de seguridad de obligado cumplimiento, la cual el empleado firmará, junto con la presente DPC y las normativas contenidas en las PC que sean de aplicación.

5.3.9. Actividades no permitidas

Salvo autorización expresa, no está permitido instalar, utilizar o solicitar información de instrumentos que puedan ser empleados para evaluar o comprometer la seguridad de los sistemas de certificación de ANF AC. Tampoco se permite la instalación o utilización, sin autorización expresa, de instrumentos que tengan como fin cualquier intento de evaluación de los servicios que utiliza o recibe ANF AC.

Esta prohibición se extiende a cualquier intento de comprobación o intento de comprometer las medidas de seguridad de ANF AC, aunque no se utilice instrumento alguno. En igual medida, se extiende a la evaluación no autorizada de los servicios prestados o recibidos de ANF AC, se empleen o no dispositivos al efecto.

También está expresamente prohibida la utilización de software o hardware que no esté expresamente autorizado por la empresa, así como la instalación, almacenaje o distribución por cualquier medio.

Queda prohibido comunicar a otra persona el identificador de usuario y la clave de acceso. Si el usuario sospecha que otra persona conoce sus datos de identificación y acceso deberá activar los mecanismos de cambio de contraseña.

El usuario está obligado a utilizar los datos, la red corporativa y/o la intranet de la entidad y/o de terceros sin incurrir en actividades que puedan ser consideradas ilícitas o ilegales, que infrinjan los derechos de la empresa y/o de terceros o que puedan atentar contra la moral o las normas de etiqueta de las redes telemáticas.

Asimismo, no está permitido:

- Compartir o facilitar el identificador de usuario y la clave de acceso facilitado por la Entidad a otra persona física o jurídica. En caso de incumplimiento de esta prohibición, el usuario será el único responsable de los actos realizados por la persona física o jurídica que utilice de forma no autorizada su identificación de usuario.
- Intentar descifrar la clave, sistemas o algoritmos de cifrado y cualquier otro elemento de seguridad que intervenga en los procesos telemáticos de la Entidad.
- Intentar leer, borrar, copiar o modificar los mensajes de correo electrónico o archivos de otros usuarios.
- Intentar distorsionar o falsear los registros log del sistema.
- Utilizar el sistema para intentar acceder a áreas restringidas de los sistemas informáticos de la Entidad y/o de terceros.
- Intentar aumentar el nivel de privilegios de un usuario en el sistema.
- Destruir, alterar, inutilizar o de cualquier otra forma dañar los datos, programas o documentos electrónicos de la Entidad o de terceros.
- El usuario no deberá almacenar datos de carácter personal en el disco duro del ordenador, sino utilizar para tal fin las carpetas de la red corporativa asignada.

- Obstaculizar voluntariamente el acceso de otros usuarios a la red mediante el consumo masivo de los recursos informáticos y telemáticos de la organización, así como realizar acciones que dañen, interrumpan o generen errores en dichos sistemas.
- Enviar mensajes de correo electrónico de forma masiva con fines comerciales o publicitarios sin el consentimiento del destinatario.
- Introducir voluntariamente programas, virus, macros, applets, componentes ActiveX o cualquier otro dispositivo lógico o secuencia de caracteres que causen o sean susceptibles de causar cualquier tipo de alteración en los sistemas informáticos de la empresa o de terceros. Al respecto, cabe recordar que el propio sistema ejecuta automáticamente los programas antivirus y sus actualizaciones para prevenir la entrada en el sistema de cualquier elemento destinado a destruir o corromper los datos informáticos.
- Introducir, descargar de Internet, reproducir, utilizar o distribuir programas informáticos no autorizados expresamente por la empresa. Esta prohibición incluye cualquier otro tipo de obra o material cuyos derechos de propiedad intelectual o industrial pertenezcan a terceros, cuando no se disponga de autorización para ello.
- Instalar copias ilegales de cualquier programa, incluidos los que están estandarizados.
- Borrar cualquiera de los programas instalados legalmente.
- Enviar o reenviar mensajes en cadena o de tipo piramidal.
- Utilizar los recursos telemáticos de la empresa, incluida la red Internet, para actividades que no se hallen directamente relacionadas con el puesto de trabajo del usuario.
- Introducir contenidos obscenos, inmorales u ofensivos y, en general, carentes de utilidad para los objetivos de la empresa.
- Cifrar información sin estar expresamente autorizado para ello.
- Acceso físico o lógico a las instalaciones de ANF AC fuera de su horario de empleo.

5.4. Procedimientos de registro de auditoría

Se utilizan los ficheros de log para reconstruir los eventos significativos que han sido realizados por el software de ANF AC, las Autoridades de Registro Reconocidas, el suscriptor o el evento que los originó. Los log son evidencias que pueden ser utilizadas como un medio de arbitraje en posibles disputas.

5.4.1. Tipos de eventos registrados

Para todos los eventos identificados en esta sección, el registro de auditoría deberá contener al menos:

- El tipo de evento registrado.
- La fecha y hora en que se ha producido.
- Descripción del evento.

- Para los mensajes de las Autoridades de Registro solicitando acciones de la Entidad de Certificación, la identificación del origen del mensaje, el destinatario y el contenido.
- Para las solicitudes de emisión o revocación de los certificados, un indicador de la concesión o la denegación de la petición.

5.4.1.1. Tipos de eventos registrados sobre el ciclo de vida del certificado y claves de CA

- Ceremonia de generación de claves y las bases de datos de gestión de claves.
- Copia de seguridad *(back up)*, almacenamiento, recuperación, archivo y destrucción de las claves.
- La instalación de las llaves criptográficas manual y sus resultados (con la identidad del operador).
- El uso de claves de la CA.
- La retirada del material de claves del servicio.
- La identidad de los encargados de manipular cualquier material asociado a las claves (como componentes de clave, dispositivos portátiles que almacenan claves, o medios de transmisión).
- La custodia de las claves, los dispositivos o medios de utilización de las claves y el posible compromiso de una clave privada.
- Generación de CRLs y entradas OCSP;
- Introducción de nuevos perfiles de certificado y retirada de perfiles de certificado existentes
- Posesión de datos de activación, para operaciones con la clave privada CA.

5.4.1.2. Tipos de eventos registrados sobre el ciclo de vida del certificado de suscriptor

- Recepción de las solicitudes de certificados, y solicitudes de renovaciones, regeneración de claves y revocaciones.
- Cómo se han generado las claves.
- Evidencias de validación de las solicitudes por los RDE, tanto para aprobación como rechazo.
- Emisión de certificados.
- Distribución de la clave pública.
- Generación y publicación de listas de revocación de certificados y entradas OCSP.

- Cambios en las políticas de emisión de certificados.

Esta CA no registra información sobre reactivación de certificados, dado que no está autorizada la suspensión temporal, y la revocación es de carácter definitivo.

5.4.1.3. Tipos de eventos registrados sobre dispositivos criptográficos

- La recepción e instalación del dispositivo.
- La conexión o desconexión de un dispositivo de almacenamiento.
- La activación del dispositivo y el uso.
- El proceso de instalación.
- La designación de un dispositivo para servicio y reparación.
- El final del ciclo de vida del dispositivo.

5.4.1.4. Tipos de eventos de seguridad registrados

- Arranque y parada de los sistemas.
- Inicio y terminación de la aplicación de emisión de certificados.
- Intentos de acceso al sistema PKI exitosos y fallidos;
- Los cambios de perfil de seguridad.
- Instalación, actualización y eliminación de software en el sistema de certificados;
- Los fallos del sistema, fallos de hardware y otras anomalías.
- Intentos de crear, borrar, cambiar contraseñas o permisos de los usuarios dentro del sistema.
- Intentos no autorizados de entrada en la red del prestador de servicios de certificación.
- Intentos no autorizados de acceso a los ficheros del sistema.
- Intentos fallidos de lectura en un certificado, y de lectura y escritura en el Repositorio de certificados.

Ya sea manual o electrónicamente, ANF AC guarda la siguiente información:

- Los registros de acceso físico, de entrada y salida.
- Mantenimientos y cambios de configuración del sistema.
- Cambios en el personal.
- Incidencias.

- Registros de la destrucción de material que contenga información de claves, datos de activación o información personal.
- Acuerdos con el suscriptor y cualquier elección específica realizada en conformidad con el suscriptor. Obra en poder de los Terceros Vinculados a disposición de la CA.

- El uso de mecanismos de identificación y autenticación, tanto autorizados como denegados (incluyendo múltiples intentos de autenticación denegados).
- Las medidas adoptadas por los individuos en roles de confianza, los operadores de computadoras, los administradores de sistemas, y los oficiales de seguridad del sistema.

5.4.2. Frecuencia de tratamiento de registros de auditoría

Los registros de auditoría son revisados periódicamente por el auditor.

El procesamiento de los registros de auditoría consiste en una revisión de los registros (verificando que éstos no han sido manipulados), una inspección aleatoria de todas las entradas de registro y una investigación más profunda de cualquier alerta o irregularidad en los registros.

Las incidencias detectadas son documentadas, detallando las medidas adoptadas y el personal implicado en la toma de decisiones.

Existe un control de acceso a las herramientas de auditoría, evitando así el uso o abuso de éstas. El uso o acceso a estas herramientas únicamente es desempeñado por las personas responsables con autorización especial.

5.4.3. Período de retención del registro de auditoría

Los registros de auditoría especificados en el apartado 5.4.1 se conservan durante toda la vigencia de la acreditación de la Entidad de Certificación. Estos registros se ponen a disposición del auditor cualificado a petición.

5.4.4. Protección de registro de auditoría

Los ficheros de registros, tanto manuales como electrónicos, están protegidos de lecturas, modificaciones, borrados o cualquier otro tipo de manipulación no autorizada, aplicando controles de acceso lógico y físico. Las claves privadas utilizadas para el registro de auditoría únicamente están destinadas a este fin.

Estas medidas de protección imposibilitan la eliminación de los registros de auditoría antes de que haya expirado su periodo de almacenamiento.

5.4.5. Procedimientos de copia de seguridad del registro de auditoría

Las copias de respaldo de los registros de auditoría se realizan según las medidas establecidas para las copias de respaldo de las Bases de Datos.

5.4.6. Sistema de recogida de información de auditorías (interno vs. externo)

Los archivos de log son almacenados en los sistemas internos, mediante una combinación de procesos automáticos y manuales ejecutados por las aplicaciones de la PKI.

Lista de riesgos contemplados:

- Inserción o alteración fraudulenta de un registro de sesión.
- Supresión fraudulenta de sesiones intermedias.
- Inserción, alteración o supresión fraudulenta de un registro histórico.
- Inserción, alteración o supresión fraudulenta del registro de una tabla de consultas.

5.4.7. Notificación al sujeto causante del evento

No aplicable. No se prevé la notificación automática de la acción de los ficheros de registro de auditoría al causante del evento.

5.4.8. Análisis de vulnerabilidad

Se realiza un análisis de vulnerabilidades periódico en los sistemas internos de ANF AC. Además, el programa de seguridad de ANF AC incluye una Evaluación y Análisis de Riesgos anual que:

1. Identifica amenazas internas y externas previsibles que podrían resultar en acceso no autorizado, divulgación, mal uso, alteración o destrucción de los Datos de certificado o Procesos de gestión de certificados;
2. Evalúa la probabilidad y el daño potencial de estas amenazas, teniendo en cuenta la sensibilidad de los Datos del Certificado y los Procesos de Gestión del Certificado; y
3. Evalúa la suficiencia de las políticas, procedimientos, sistemas de información, tecnología y otros acuerdos que ANF AC tiene para contrarrestar dichas amenazas.

5.5. Archivo

Toda la información relativa a los certificados se guarda durante un período de tiempo apropiado, según lo establecido en la sección 5.5.2 de este documento.

Se debe destacar que, en relación a la documentación confidencial, ANF AC no utiliza en su actividad de trabajo documentos en soporte papel. Todos los documentos son desmaterializados, codificados según nivel de seguridad, y almacenados en repositorios seguros creados a tal fin.

El soporte papel es almacenado en almacenes cerrados, sólo accesibles a personal expresamente autorizado, y que cuentan de seguridad permanente 24/7/365, con sistema de monitorización y alarmas.

5.5.1. Tipos de registros archivados

ANF AC guarda todos los eventos que tengan lugar durante el ciclo de vida de un certificado, incluyendo la renovación del mismo.

El prestador de servicios de certificación tiene que guardar un registro de, al menos, la siguiente información:

- Datos relacionados con el procedimiento de registro y solicitud de certificados.
- Los registros de auditoría especificados en este documento.
- Incidencias detectadas.

- El método de identificación aplicado.
- Registro de los datos de identificación únicos (por ejemplo, cédula de identidad o documentos de identificación, en su caso).
- Copia digitalizada y firmada por el Tercero Vinculado, de los documentos presentados por el suscriptor.
- Identidad del operador AR que tramita la solicitud.
- Lugar de almacenamiento de copias de solicitudes y documentos de identificación.
- La identidad del operador que acepta la solicitud.
- Método utilizado para validar los documentos de identificación.
- Nombre e identificador del Tercero Vinculado que realiza la tramitación.
- La aceptación del suscriptor del Acuerdo de Suscripción, el consentimiento del suscriptor para permitir que la CA mantenga en sus repositorios los registros que contienen datos de carácter personal, la posible autorización para el acceso de terceros a estos registros, y la publicación de los certificados.
- Lugar de almacenamiento de copias de solicitudes y documentos de identificación.

5.5.2. Periodo de retención para archivo

ANF AC conserva todos los registros indicados en la sección anterior de manera íntegra, durante toda la vigencia de la acreditación de la Entidad de Certificación y siempre conforme a lo establecido por la legislación vigente.

5.5.3. Protección de archivo

Se adoptan las medidas de protección del archivo, para que no pueda ser manipulado ni destruido su contenido. ANF protege sus ficheros de datos de carácter personal de acuerdo con lo previsto en el apartado 9.4.1 del presente documento.

5.5.4. Procedimientos de copia de seguridad de archivo

ANF AC realiza copias de respaldo incrementales diarias de todos sus documentos electrónicos, además se realizan copias de respaldo completas semanalmente, y se custodian copias históricas mensuales.

Existe una política de copias de seguridad que definen los criterios y estrategias de actuación ante una incidencia.

5.5.5. Requisitos para el sellado de tiempo de los registros

Los sistemas de información empleados por ANF AC garantizan el registro del tiempo en los que se realizan. El instante de tiempo de los sistemas proviene de una fuente segura que constata la fecha y hora.

En concreto, la señal de reloj es sincronizada con el Real Instituto y Observatorio de la Armada - San Fernando (Cádiz), “ROA”, que es el responsable del mantenimiento de la unidad básica de Tiempo, declarado a efectos legales como Patrón Nacional de dicha unidad, así como del mantenimiento y difusión oficial de la escala “Tiempo Universal Coordinado” (UTC(ROA)), considerada a todos los efectos como la base de la hora legal en todo el territorio nacional (R.D. 23 octubre 1992, núm. 1308/1992).

Este laboratorio mantiene en funcionamiento varios servidores que distribuyen el tiempo a través del protocolo NTP. Este sistema de alta estabilidad y precisión utiliza un conjunto de patrones atómicos de cesio, que permiten conocer el tiempo UTC con una precisión superior al microsegundo, y con una estabilidad de 32 s/año.

Al menos una vez al día todos los sistemas se sincronizan con esta fuente.

Para efectos legales el servicio de sellado de tiempo se prestará tomando como referencia el huso horario del territorio continental ecuatoriano UTC ("Universal Time Coordinated").

5.5.6. Sistema de recogida de archivos (interno o externo)

El sistema de recogida de información es interno y corresponde a ANF AC.

5.5.7. Procedimientos para obtener y verificar información de archivo.

El acceso a esta información está restringido al personal autorizado a tal efecto, protegiéndose frente a accesos físicos y lógicos.

5.6. Cambio de claves de CA (Key changeover)

Con anterioridad a la expiración del periodo de vigencia del certificado de una CA raíz o subordinada, se procederá a la creación de una nueva CA raíz o subordinada correspondiente, mediante la generación de un nuevo par de claves. Se podrán introducir cambios en el contenido del certificado que se ajusten mejor a la legislación vigente, a la PKI de ANF AC y a la realidad del mercado. Las CA antiguas y sus claves privadas asociadas únicamente se usarán para la firma de CRLs y ARL mientras existan certificados activos emitidos por dicha CA.

Los procedimientos para proporcionar, en caso de cambio de claves de una CA, la nueva clave pública de CA a los titulares y terceros aceptantes de los certificados de la misma son los mismos que para proporcionar la clave pública en vigor. Se publicará en el sitio web https://crl.anf.es/

La documentación técnica y de seguridad de la CA detalla el proceso de cambio de claves de la CA.

5.7. Compromiso y recuperación ante desastres

5.7.1. Procedimientos de manejo de incidencias y compromisos

Existe un Plan de Continuidad de Negocio y Recuperación de Desastres, OID 1.3.6.1.4.1.37442.13.1.1, que define las acciones a realizar, recursos a utilizar y personal a emplear en el caso de producirse un acontecimiento intencionado o accidental que inutilice o degrade los recursos y los servicios de certificación de ANF AC. Los principales objetivos del Plan de Continuidad de Negocio y Recuperación de Desastres son:

- Maximizar la efectividad de las operaciones de recuperación mediante el establecimiento de tres fases:
    - Fase de Notificación/Evaluación/Activación para detectar, evaluar los daños y activar el plan.
    - Fase de Recuperación para restablecer temporal y parcialmente los servicios hasta la recuperación de los daños provocados en el sistema original.
    - Fase de Reconstitución para restaurar el sistema y los procesos a su operativa habitual.
- Identificar las actividades, recursos y procedimientos necesarios para la prestación parcial de los servicios de certificación.
- Asignar responsabilidades al personal designado por el Comité de Seguridad y facilitar una guía para la recuperación de la operativa habitual.

- Asegurar la coordinación de todos los operadores que participen en la estrategia de contingencia planificada.

La evaluación de los daños y el plan de acción se describen en el Plan de Continuidad de Negocio y Recuperación de Desastres.

Se Informará a los suscriptores y otras entidades con las que el ANF AC tiene acuerdos o relación en caso de compromiso.

En el caso de producirse la circunstancia de debilidad del sistema criptográfico: el algoritmo, la combinación de los tamaños de clave utilizados o cualquier otra circunstancia técnica que debilite significativamente la seguridad técnica del sistema, se aplicará lo definido en el Plan de Continuidad de Negocio y Recuperación de Desastres.

5.7.2. Alteración de los recursos de computación, hardware y software

Cuando tenga lugar un evento de corrupción de recursos, aplicaciones o datos, se activará un procedimiento que permita iniciar las gestiones necesarias, de acuerdo con el Plan de Continuidad de Negocio y Recuperación de Desastres, que recoge la estrategia de actuación ante este tipo de situaciones.

5.7.3. Procedimientos de compromiso de la clave privada de la CA o de la suite criptográfica

El Plan de Continuidad de Negocio de ANF AC contempla el compromiso o la sospecha de compromiso de la clave privada de una CA como un desastre.

En caso de compromiso de una CA intermedia o subordinada, debe realizar como mínimo las siguientes acciones:

- Verificar el compromiso y, en caso de confirmación, informar a todos los suscriptores.
- Indicar que los certificados y la información del estado de revocación que han sido entregados usando la clave de esta CA ya no son válidos.
- Proceder en conformidad con lo indicado en el apartado 4.9.11

En el supuesto de que la clave comprometida sea la de la CA raíz, se eliminará el certificado de todas las aplicaciones y se distribuirá uno nuevo.

El Plan de Continuidad del Negocio de ANF AC establece que, en caso de compromiso de la clave de la CA, el certificado asociado será inmediatamente revocado, e igualmente serán revocados todos los certificados que hayan sido emitidos con ese certificado, ofreciendo a las entidades finales la posibilidad de disponer de un nuevo certificado emitido por una nueva CA, gratuitamente y por un periodo de tiempo igual al que restaba de vida.

Asimismo, se ofrecerá un servicio de retimbrado gratuito de los documentos firmados con los certificados revocados.

En caso de **revocación** de una de las Jerarquías de Certificación de ANF AC, se llevará a cabo lo siguiente:

- Notificar este hecho, cuando se produzca, a la ARCOTEL.
- Informar del hecho publicando una ARL.
- Realizar todos los esfuerzos necesarios para informar de la revocación a todos los suscriptores a los cuales el prestador de servicios de certificación emitió certificados, así como a los terceros que deseen confiar en esos certificados.

- Realizar una renovación de claves y llevar a cabo una transmisión electrónica de ésta, en caso de que la revocación no haya sido debida a la terminación del servicio por parte del prestador de servicios de certificación, según lo establecido en esta DPC.

Las causas de revocación contempladas en el presente apartado pueden ser por compromiso de clave, causas técnicas, razones organizativas o desastre.

ANF AC dispone de un Plan de Continuidad del Negocio y Recuperación de Desastres, que será aplicado en el caso de que los avances de la técnica pongan en riesgo la seguridad técnica de los algoritmos, el tamaño de clave utilizado o cualquier otra circunstancia técnica. En caso de posible riesgo, se realizará un análisis de impacto. En ese análisis se estudiará la criticidad del problema de seguridad, su ámbito y la estrategia de recuperación ante la incidencia.

Los puntos mínimos que debe de incluir el informe de análisis de impacto son:

- Descripción detallada de la contingencia, ámbito temporal, etc.
- Criticidad, ámbito.
- Soluciones propuestas.
- Plan de despliegue de la solución elegida, que incluirá al menos:
    - Notificación a los usuarios, tanto a los suscriptores como a los terceros que confían.
    - Se informará en la web de la contingencia producida
    - Revocación de los certificados afectados
    - Estrategia de renovación

5.7.4. Capacidad de continuidad de negocio después de un desastre

El Plan de Continuidad de Negocio y Recuperación de Desastres de ANF AC desarrolla, mantiene y contempla la posibilidad de probar y, si es necesario, ejecutar un plan de emergencia para el caso de que ocurra un desastre, ya sea por causas naturales o humanas, sobre las instalaciones, el cual indica cómo restaurar los servicios de los sistemas de información.

Los sistemas e instalaciones definidas en Plan de Continuidad de Negocio y Recuperación de Desastres disponen de las protecciones físicas exigibles.

El Plan de Continuidad de Negocio y Recuperación de Desastres de ANF AC establece la capacidad de restaurar la operación normal de los servicios de revocación y, en su caso, de suspensión, en las 24 horas siguientes al desastre, pudiendo, como mínimo, ejecutarse las siguientes acciones:

- Revocatoria de certificados (en su caso).
- Publicación de información de revocación.

La base de datos de recuperación de desastres utilizada por los servicios de certificación de ANF AC está sincronizada con la base de datos de producción dentro de los límites temporales especificados en el plan de seguridad.

Los equipos de recuperación de desastres de servicios de certificación de ANF AC tienen las medidas de seguridad físicas especificadas en el plan de seguridad.

5.8. Cese de CA o del Tercero Vinculado

5.8.1. Cese de la CA

ANF AC sigue las recomendaciones expresadas en las normas de referencia.

Con el fin de minimizar los efectos a los Terceros Vinculados, a los suscriptores y a terceras partes como consecuencia del cese en la prestación de servicios. ANF AC se compromete a llevar a cabo, como mínimo, los siguientes procedimientos:

- Notificar con al menos noventa días de anticipación a los titulares de los certificados de firma electrónica, a los Terceros Vinculados y a los organismos de regulación y control sobre la terminación de sus actividades.
- Informar a todos los suscriptores y terceros que confían en los certificados que han emitido. Para ello hará, durante un periodo de noventa días, la correspondiente publicación en la página principal de la web corporativa.
- Retirar toda autorización de subcontrataciones que actúan en nombre del prestador de servicios de certificación en el proceso de emisión de certificados, incluidos los Terceros Vinculados.
- Ejecutar las tareas necesarias para transferir las obligaciones de mantenimiento de la información de registro y los archivos de registro de eventos, durante los períodos de tiempo respectivos indicados al suscriptor y a los terceros que confían.
- Destruir las claves privadas de todas las CA.
- Revocar todos los certificados de las CA emitidos.
- Adoptar las medidas necesarias para garantizar la continuidad de los servicios de certificación mediante la transferencia de la gestión de los certificados que sigan siendo válidos en la fecha de cese a otra Entidad de Certificación informando previamente a los suscriptores y a la ARCOTEL sobre la identidad y características del nuevo prestador, y obteniendo autorización expresa del titular del certificado.

En el caso de que no sea traspasada la actividad a otra entidad de certificación o el titular no autorice ese proceso:

- El certificado será revocado de forma anticipada.
- Se mantendrán en línea las listas de certificados revocados por un periodo no inferior a cinco años.
- Se realizará depósito notarial público, de las listas de certificados revocados y de los medios necesarios para verificar la validez de los certificados y firmas electrónicas elaboradas con ellos.

5.8.2. Cese del Tercero Vinculado

El marco de colaboración de ANF AC con sus Terceros Vinculados está formalizado mediante el correspondiente contrato que contempla sus “Obligaciones y Responsabilidades”. El Tercero Vinculado, formalmente, se compromete entre otras cuestiones a:

- Notificar con al menos treinta días de anticipación a ANF AC, sobre la terminación de su actividad.
- Cesar su actividad como AR en el mismo momento en el que comunica su intención de cesar en su actividad, o en el momento en el que ANF AC le comunique la revocación de su acreditación como Tercero Vinculado. De forma inmediata comunicará la correspondiente orden de cese de la actividad a todos sus Operadores AR.
- Dentro de los treinta días desde que se efectúo la notificación de cese de actividad, el Tercero Vinculado procederá a hacer entrega a ANF AC de todo el material relacionado con la actividad desarrollada como Autoridad de Registro (AR), suprimiendo de sus archivos físicos e informáticos de cualquier información y contenido relacionado con su labor como AR.
- Prestar máxima colaboración y transparencia en caso de ser requerido para realizar una auditoría interna de seguridad que garantice que todas las obligaciones como Tercero Vinculado han sido atendidas adecuadamente.

5.8.2.1. Cese de un Operador AR

El marco de colaboración de ANF AC con los Operadores AR, está formalizado mediante el correspondiente contrato que contempla sus "Obligaciones y Responsabilidades". El Operador AR, formalmente se compromete entre otras cuestiones a:

- Notificar con al menos quince días de anticipación al Tercero Vinculado al que está adscrito, sobre la terminación de su actividad como Operador AR.
- Cesar su actividad como Operador AR en el mismo momento en el que comunica su intención de cesar en su actividad, en el momento en el que el Tercero Vinculado del que depende así se lo ordene, o en el momento en el que ANF AC le comunique la revocación de su acreditación como Operador AR.
- Dentro de los quince días desde que se efectúe la notificación de cese de actividad, el Operador AR procederá a hacer entrega al Tercero Vinculado al que está adscrito todo el material relacionado con la actividad desarrollada como Operador AR.
- Prestar máxima colaboración y transparencia en caso de ser requerido para realizar una auditoría interna de seguridad que garantice que todas las obligaciones como Operador AR han sido atendidas adecuadamente.

6. CONTROLES DE SEGURIDAD TÉCNICA

ANF AC emplea sistemas y productos fiables, que están protegidos contra toda alteración y que garantizan la seguridad técnica y criptográfica de los procesos de certificación a los que sirven de soporte.

Para el desarrollo de su actividad como Entidad de Certificación de Información y Servicios Relacionados Acreditada, ANF AC cuenta con un Departamento de I+D+i, y una sección criptográfica que determina el estado de seguridad de todos los elementos criptográficos utilizados en su PKI.

6.1. Generación e instalación del par de claves

6.1.1. Generación de pares de claves

6.1.1.1. Generación del par de claves de CA / VA / TSA

Las claves criptográficas de la CA raíz y subordinadas deben ser generadas en un módulo hardware criptográfico (HSM) que cumpla con FIPS 140-2 nivel 3 (o superior) y Common Criteria EAL 4+ sobre el perfil de protección correspondiente.

Las claves criptográficas de la VA deben ser generadas en un módulo hardware criptográfico (HSM) que cumpla con FIPS 140-2 nivel 3 (o superior) y Common Criteria EAL 4+ sobre el perfil de protección correspondiente.

Las claves criptográficas de la TSA deben ser generadas en un módulo hardware criptográfico (HSM) que cumpla con FIPS 140-2 nivel 3 (o superior) y Common Criteria EAL 4+ sobre el perfil de protección correspondiente.

ANF AC garantiza que el módulo hardware criptográfico utilizado, en concordancia con los anteriores apartados, no ha sido manipulado durante el envío, recepción, ni su almacenamiento. Por otro lado, la instalación, activación, copias de seguridad y recuperación de las claves en el módulo hardware criptográfico necesita del control simultáneo de dos empleados de confianza de ANF AC. Asimismo, ANF AC garantiza que las claves de firma de la CA almacenadas en el hardware criptográfico se destruyen al retirarse el dispositivo; esta destrucción no afecta a todas las copias de la clave privada, sólo a la clave almacenada en el hardware criptográfico en cuestión.

Las claves criptográficas de CA, VA, TSA y usuarios finales deben ser generadas siguiendo las recomendaciones de algoritmo y longitud de clave mínimas definidas en ETSI TS 119 312.

6.1.1.2. Generación del par de claves del suscriptor

En los sistemas de Infraestructura de Clave Pública (PKI por sus siglas en inglés), toda la robustez del sistema pesa sobre la protección de la clave privada, asegurando que ésta ha estado únicamente en manos del suscriptor, al contrario que la clave pública, que como bien indica su nombre, puede ser distribuida libremente y mediante la cual los terceros podrán verificar las firmas del suscriptor, y cifrar mensajes que solo el suscriptor podrá leer. La clave privada realiza las funciones inversas, permite firmar documentos y descifrar datos, es por ello que hay que resguardar su seguridad.

En el caso de certificados en modalidad software criptográfico, ANF AC entrega a los suscriptores el software criptográfico necesario para generar en privado y sin intervención de terceros, su par de claves y los datos de activación de las mismas. Esto garantiza el cumplimiento de los parámetros y tamaños seguros de la clave. En aquellos casos en los que ANF AC genere las claves criptográficas de sus usuarios (solo aplicable modalidad software), ANF AC garantiza la confidencialidad durante el proceso de generación de dichos datos, y la seguridad en su transmisión al sujeto.

En el caso de certificados en modalidad DSCF, ANF AC proporciona a los suscriptores de un Dispositivo Seguro de Creación de Firma (DSCF). Los dispositivos seguros de creación de firma suministrados por ANF AC a sus suscriptores, son dispositivos QSCD o SSCD publicados oficialmente por la Comisión Europea o dispositivos con nivel de seguridad FIPS 140-2 nivel 3 o superior. ANF AC también proporciona al titular del certificado el software criptográfico necesario para generar en privado y sin intervención de terceros, su par de claves y los datos de activación de las mismas. En los casos en que ANF AC pueda garantizar que las claves criptográficas del firmante fueron creadas en DSCF, ANF AC incluirá el identificador OID correspondiente en la extensión "Certificate Policies".

En el ámbito de certificados electrónicos de firma centralizada, ANF AC para la generación de las claves, su almacenamiento y posterior uso en el ámbito de firma centralizada, utiliza exclusivamente dispositivos certificados incluidos en la lista de dispositivos cualificados mantenida por la Comisión Europea,

https://ec.europa.eu/futurium/en/content/compilation-member-states-notification-sscds-and-qscds

Además, ANF AC pone a disposición de los suscriptores canales de comunicación segura y procedimientos de seguridad de la gestión y administrativos específicos.

6.1.2. Entrega de clave privada al suscriptor

Es el suscriptor quien se genera y está en posesión de la clave privada.

En aquellos casos en los que ANF AC genere las claves criptográficas de sus usuarios, el procedimiento de entrega de la clave privada variará en función del tipo de certificado y dispositivo. Cada Política de Certificación especifica el método empleado.

6.1.3. Entrega de claves públicas al emisor del certificado

La clave pública es generada por el suscriptor y es entregada a ANF AC mediante el envío de una solicitud de certificación en formato CSR (Certificate Signing Request), que sigue la especificación PKCS#10.

6.1.4. Entrega de claves públicas de CA a terceros que confían

La clave pública de la CA Raíz y de las CA Intermedias está a disposición de los terceros que confían, asegurando la integridad de la clave y autenticando su origen.

La clave pública de la CA Raíz se publica en el Repositorio, en forma de certificado autofirmado en el caso de CA Raíz y de certificado emitido por la CA Raíz en caso de CA Intermedia, junto a una declaración que especifica que la clave es auténtica a ANF AC.

Se incluyen medidas adicionales para confiar en el certificado autofirmado, como la comprobación de la huella digital del certificado que aparece publicada en esta DPC. Los usuarios pueden acceder al Repositorio para obtener las claves públicas de ANF AC a través de la web https://www.anf.ec

6.1.5. Tamaños de clave

El algoritmo usado es RSA con SHA256. El tamaño de las claves, dependiendo de los casos, es:

Tipo de certificado	Tamaño claves RSA (bits)
CA Raíz	4096
CA Intermedia	4096
Usuario final	2048
OCSP Responder	2048
TSU	2048

6.1.6. Parámetros de generación de la clave pública y verificación de la calidad

Se utilizan los parámetros recomendados en el estándar ETSI TS 119 312. Concretamente:

Signature Suite	Función Hash	Esquema de padding	Algoritmo de firma
sha256-with-rsa	sha256	emsa-pkcs1-v1.5	rsa

ANF AC emplea algoritmos y parámetros criptográficos adecuados, siguiendo las recomendaciones del CA/B Forum y los estándares ETSI TS 119 312. Las claves públicas de los certificados se codifican conforme a RFC 5280 y PKCS#1, garantizando su seguridad e interoperabilidad.

6.1.7. Fines de uso de la clave (según el campo de uso de la clave X.509 v3)

Todos los certificados incluyen la extensión Key Usage y Extended Key Usage, indicando los usos habilitados de las claves.

Las claves de CA raíz se utilizan para firmar los certificados de las CAs subordinadas, ARLs y certificados para la verificación de respuesta OCSP; NUNCA certificados de usuario final. Las claves de las CA subordinadas o emisoras únicamente se utilizan para firmar certificados de usuario final y CRLs.

Los usos admitidos de clave para certificados finales están definidos en las Políticas de Certificación correspondientes.

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

6.2.1. Módulos criptográficos y controles

ANF AC requiere que los token HSM sean dispositivos QSCD o SSCD publicados oficialmente por la Comisión Europea o dispositivos con nivel de seguridad FIPS 140-2 nivel 3 o superior.

El módulo de seguridad criptográfico (token HSM) es un dispositivo certificado que genera y protege claves criptográficas. ANF AC mantiene protocolos para comprobar que el módulo HSM no ha sido manipulado durante su transporte y almacenamiento.

La norma europea de referencia para los dispositivos de suscriptor utilizados es la Decisión de Ejecución (UE) 2016/650 de la Comisión del 25 de abril de 2016.

ANF AC mantiene el control sobre la preparación, almacenamiento y distribución de los dispositivos de usuario final, pero la generación de las claves las realiza el propio usuario.

Existe un documento de Ceremonia de Generación de Claves de la CA raíz y CAs Intermedias, donde se describen los procesos de generación de la clave privada y el uso del hardware criptográfico.

ANF AC para la generación de las claves de las CAs respeta las recomendaciones de ETSI EN 319 411-1, y CAB / Forum Baseline Requirement Guidelines. Por otro parte, ANF AC garantiza que las claves utilizadas para generar certificados, y/o para emitir información sobre estados de revocación, no serán utilizadas para ningún otro propósito, y una vez alcancen el final de su ciclo vida, todas las claves privadas de firma de la CA serán destruidas o inutilizadas.

Además, el uso de la clave privada de la CA se limitará a la que sea compatible con el algoritmo hash, el algoritmo de firma y la longitud de clave de firma utilizados en la generación de certificados, en concordancia con la ETSI TS 102 176 "Technical Specification Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures".

6.2.2. Control multi-persona (n de m) de la clave privada

La utilización de las claves privadas de las CA's requiere la intervención de al menos dos de los operadores autorizados.

6.2.3. Custodia de clave privada

La clave privada de la CA raíz y CA Intermedia están depositadas en un dispositivo criptográfico hardware certificado con la norma FIPS 140-2 nivel 3 y/o CC EAL4+ (o superior), garantizando que la clave privada nunca está fuera del dispositivo criptográfico.

Las claves privadas de la CA raíz serán mantenidas y utilizadas aisladas físicamente de las operaciones normales de tal manera que sólo personal de confianza designado tenga acceso a las claves para su uso en la firma de certificados de CA subordinada.

Los dispositivos de usuario final están bajo su custodia, y éste será el responsable de mantenerla bajo su exclusivo control.

Por otro lado, en el ámbito de certificados electrónicos de firma centralizada, ANF AC, para la generación de las claves, su almacenamiento y posterior uso en el ámbito de firma centralizada, utiliza exclusivamente dispositivos certificados incluidos en la lista de dispositivos cualificados mantenida por la Comisión Europea,

https://ec.europa.eu/futurium/en/content/compilation-member-states-notification-sscds-and-qscds

Además, ANF AC pone a disposición de los suscriptores, procedimientos y mecanismos adecuados para garantizar que el firmante tiene el control exclusivo del uso de sus datos de creación de la firma electrónica y que la utilización del dispositivo cumple los requisitos de la firma electrónica cualificada.

6.2.4. Copia de seguridad de clave privada

Existe un procedimiento de recuperación de claves de los módulos criptográficos de la CA (raíz o intermedias) que se puede aplicar en caso de contingencia, y que es aplicado durante la Ceremonia de Emisión de Certificados de CA.

Existe un procedimiento de recuperación de claves de los módulos criptográficos de los suscriptores que hayan contratado a ANF AC la custodia de las claves, que se puede aplicar en caso de contingencia.

6.2.5. Archivo de clave privada

Ver apartado 6.2.3.

6.2.6. Transferencia de clave privada hacia o desde un módulo criptográfico

Ver apartado 6.2.7.

6.2.7. Almacenamiento de claves privadas en módulo criptográfico

Sólo en el caso de contingencia se utiliza el procedimiento indicado en el apartado 6.2.4 para introducir la clave privada en los módulos criptográficos.

6.2.8. Método de activación de la clave privada

En todos los casos se requiere el empleo de datos de activación de firma (PIN) para utilizar las claves privadas de los dispositivos criptográficos. Se entrega por un sistema que permite mantener la confidencialidad necesaria.

Las claves de la CA Raíz y de las CAs subordinadas se activan por un proceso que requiere la utilización simultánea de al menos dos dispositivos criptográficos HSM (SmartCards).

El acceso a la clave privada del suscriptor depende del dispositivo en el que esté generada. Cada usuario recibe un manual de uso.

6.2.9. Método de desactivación de la clave privada

La extracción del dispositivo criptográfico del equipo emisor supone la finalización de cualquier acción de operación en curso.

Las claves de la CA Raíz, y las CAs subordinadas, se desactivan al estar la sesión sin actividad durante un tiempo determinado.

En dispositivos de usuario final depende del dispositivo en el que esté generada, pero como regla general es responsabilidad del suscriptor desactivar el acceso a la clave privada.

6.2.10. Método de destrucción de la clave privada

ANF AC dispone de un procedimiento de destrucción de claves de la CA según las instrucciones del fabricante del módulo criptográfico de seguridad.

En el caso de claves privadas en dispositivos de usuario final, los dispositivos criptográficos que contienen las claves privadas creadas por los suscriptores incorporan un procedimiento de destrucción de claves.

Por otro lado, en el ámbito de certificados electrónicos de firma centralizada, ANF AC dispone de un procedimiento de destrucción de la clave privada de los suscriptores que así se lo soliciten. El suscriptor que requiera la destrucción de su clave privada deberá identificarse personalmente ante ANF AC, o uno de sus Terceros Vinculados, notario público o realizar la petición mediante documento firmado electrónicamente.

6.2.11. Clasificación del módulo criptográfico

Ver apartado 6.2.1.

6.3. Otros aspectos de la gestión del par de claves

6.3.1. Archivo de clave pública

Los certificados generados por la CA, son almacenados durante toda la vigencia de la acreditación. Asumiendo con posterioridad las obligaciones legales que le apliquen.

6.3.2. Periodos operativos de certificados y períodos de uso de pares de claves

Es el periodo de vigencia de cada uno de los certificados, y se encuentra especificado en cada uno de ellos.

6.4. Datos de activación

6.4.1. Generación e instalación de datos de activación

Los datos de activación de las claves de la CA Raíz y de las CAs subordinadas se generan durante la Ceremonia de Creación de la CA raíz y CA subordinada.

La generación e instalación de los datos de activación de la clave privada del suscriptor depende del dispositivo:

- **Certificados de identidad emitidos en dispositivo criptográfico:** En todos los casos,
    - Se entrega al operador autorizado a utilizar el dispositivo criptográfico, un sistema que permite mantener la confidencialidad y libre elección de los datos de activación de firma (PIN).
    - El PIN es generado por el operador autorizado del dispositivo criptográfico durante el proceso de creación de las claves.
    - El dispositivo criptográfico emplea una lógica de seguridad que sólo permite la elección de datos de activación (PIN) que cumplen unos requerimientos básicos de seguridad.
    - El dispositivo criptográfico incorpora una función que permite al operador autorizado el cambio del PIN.
    - El PIN nunca se almacena, ni queda anotado en impreso alguno.
- **Certificados técnicos de entidad final**

  Emitidos en soporte software: la instalación y puesta en marcha de la clave privada asociada a los certificados, requiere la utilización de los sistemas de seguridad que el propio usuario haya definido. ANF AC no controla ni puede definir el modo de acceso a la clave privada en estos casos.

En el ámbito de certificados electrónicos de firma centralizada, ANF AC requerirá a los usuarios un control de doble autenticación más su PIN de activación de firma.

6.4.2. Protección de datos de activación

Los datos de activación de las claves de la CA raíz y CA Intermedias están distribuidas en múltiples tarjetas físicas, siendo necesarias al menos dos personas para realizar cualquier operación. Las claves de las tarjetas están custodiadas en la caja fuerte de ANF AC.

Las claves de la TSA y VA están generadas y gestionadas en un dispositivo HSM y se aplican las mismas reglas que en el caso de CA Raíz y CA Intermedias.

Los usuarios finales están obligados a mantener en secreto sus datos de activación.

6.4.3. Otros aspectos de los datos de activación

No se estipula el tiempo de vida de los datos de activación.

Ver Política específica de cada tipo de certificado.

6.5. Controles de seguridad informática

6.5.1. Requisitos técnicos específicos de seguridad informática

Para la identificación de terminales y, en especial, de equipos portátiles, se ha establecido un modelo según la ubicación del terminal, y en conformidad con la sensibilidad de los servicios a los que se pretende acceder:

- **Acceso local**: La identificación se realiza mediante autenticación basada en tecnología de firma electrónica, accediendo por IP interna y control de autorización previa de la MAC de la terminal.
- **Acceso remoto:** Sólo es posible acceder a equipos configurados para este fin, y según sensibilidad del servicio, está restringido el acceso a determinadas IP previamente autorizadas.

Existen una serie de controles en el emplazamiento de los diferentes elementos del sistema de prestación de servicio de certificación de ANF AC (CA, BBDD, Servicios de Telecomunicaciones, Operación CA y Gestión de Red):

- Existe un Plan de Continuidad de Negocio y Recuperación de Desastres.
- Controles operacionales:
    - Todos los procedimientos de operación están debidamente documentados en los correspondientes manuales de operación.
    - Están implantadas herramientas de protección contra virus y códigos malignos.
    - Se lleva a cabo un mantenimiento continuado del equipamiento, con el fin de asegurar su disponibilidad e integridad continuadas.
    - Existe un procedimiento de salvado, borrado y eliminación segura de soportes de información, medios removibles y equipamiento obsoleto.
- Intercambios de datos. Los siguientes intercambios de datos van cifrados para asegurar la debida confidencialidad:
    - Transmisión de datos entre los Servidores de Confianza de ANF AC y los Terceros Vinculados.
    - Transmisión de datos entre los Servidores de Confianza de ANF AC y los suscriptores de ANF AC.
- El servicio de publicación de revocaciones posee las funcionalidades necesarias para que se garantice un funcionamiento 24x7x365.
- Control de accesos:
    - Se utilizarán certificados de identidad, de forma que los usuarios están relacionados con las acciones que realizan y se les puede responsabilizar de sus acciones.

- La asignación de derechos se lleva a cabo siguiendo el principio de concesión mínima de privilegios.
- Eliminación inmediata de los derechos de acceso de los usuarios que cambian de puesto de trabajo o abandonan la organización.
- Revisión periódica del nivel de acceso asignado a los usuarios.
- La asignación de privilegios especiales se realiza "caso a caso" y se suprimen una vez terminada la causa que motivó su asignación.
- Existen directrices para garantizarla calidad en las contraseñas.

ANF AC dispone de una Política de Seguridad y procedimientos específicos para garantizar la seguridad a diferentes niveles.

Por otro lado, en el ámbito de certificados electrónicos de firma centralizada, se seguirá el mismo procedimiento detallado en este apartado.

6.5.2. Calificación de seguridad informática

Los productos utilizados para la emisión de certificados disponen de certificación de conformidad como mínimo el criterio FIPS 140-2 Nivel 3 o Common Criteria EAL 4+ para el perfil de protección correspondiente.

6.6. Controles técnicos del ciclo de vida

Para el desarrollo de su actividad, ANF AC ha implementado un sistema de gestión de seguridad de la información para los procesos de operación y mantenimiento de la infraestructura, expedición, validación y revocación de certificados electrónicos según el estándar ISO 27001.

ANF AC dispone de una Política de Seguridad de la Información, aprobada por la Junta Rectora de la PKI y que establece el enfoque de la organización para administrar su seguridad de la información. El intervalo máximo entre dos verificaciones de este documento es de un año. Los cambios en la política de seguridad de la información se comunicarán a terceros, cuando corresponda.

6.6.1. Controles de desarrollo del sistema

ANF AC realiza análisis de requisitos de seguridad durante las fases de diseño y especificación de requerimientos de cualquier componente empleado en las aplicaciones de esta PKI, a fin de garantizar que los sistemas son seguros.

Se emplean procedimientos de control de cambios para las nuevas versiones, actualizaciones y parches de emergencia de dichos componentes. Se controla la implantación de software en los sistemas de producción.

Para evitar posibles incidencias en los sistemas, se establecen los siguientes controles:

- Existe un procedimiento formal de autorización para la actualización de las librerías de software (incluyendo parches) en producción.
- Previa a la puesta en explotación del software, éste se instala en un entorno de test, donde se realizan las pruebas pertinentes.
- Se mantiene un fichero log (registro) de todas las actualizaciones de las librerías.

- Se mantienen las versiones previas del software.
- En procesos que afectan a la seguridad de los sistemas de certificación, no se instala software del que el Dpto. de Ingeniería no disponga del código fuente, y haya realizado la correspondiente comprobación de seguridad en presencia de la Dirección Técnica.

6.6.1.1. Controles en entorno de pruebas

ANF AC realiza análisis de requisitos de negocio durante las fases de diseño y especificación de cualquier componente empleado en las aplicaciones de esta PKI, a fin de garantizar que los sistemas son seguros.

Se emplean procedimientos de control de cambios en el entorno de pruebas, y se sigue un procedimiento estrictamente controlado por el responsable de sistemas del entorno de test.

Cada usuario es identificado al acceder al entorno de igual forma que en el de producción. Las nuevas versiones, actualizaciones y parches de emergencia de dichos componentes, se ejecutan siempre previamente en el entorno de pruebas y se revisan bajo el procedimiento de control de cambios.

Para evitar posibles incidencias en los sistemas, se establecen los siguientes controles:

- Existe un procedimiento formal de autorización para la actualización de las librerías de software (incluyendo parches) en test.
- El entorno test es una réplica al entorno de producción, tanto a nivel de hardware como de software.
- Existen los mismos controles de acceso al entorno que existen en el entorno real.
- Los datos que hay en el entorno test son datos de pruebas, generados por el departamento de ingeniería.
- De forma previa a la puesta en explotación del software, este es validado en el entorno de test, donde se realizan las pruebas pertinentes.
- Se mantiene un fichero log (registro) de todas las actualizaciones de las librerías.
- Se mantienen las versiones previas del software, por si existe necesidad de recuperación del sistema.
- En procesos que afectan a la seguridad de los sistemas de certificación, no se instala software del que el Dpto. de Ingeniería no disponga del código fuente, y haya realizado la correspondiente comprobación de seguridad en presencia de la Dirección Técnica.

6.6.1.2. Procedimientos de control de cambios

Se emplean procedimientos de control de cambios del desarrollo de los accesos a las bibliotecas que mantienen el software de las aplicaciones (a través de un control de versiones). Cada empleado es identificado por un ID único y queda registrada cualquier modificación, lectura, descarga o carga de código en la biblioteca.

Se mantiene así un control sobre el acceso al código fuente del programa. Asimismo, para evitar posibles incidencias, se establecen los siguientes controles:

- Existe un procedimiento formal de autorización para la actualización de las librerías de software (incluyendo parches) en test.
- De forma previa a la puesta en explotación del software, éste se instala en un entorno de test, donde se realizan las pruebas pertinentes.
- Son desechados los cambios de ficheros o desarrollos independientes que no siguen las políticas de negocio de ANF AC.
- La compra o modificación de software se controla, se autentifica el procedimiento de este y se versiona en la aplicación de control de versiones.
- Se mantiene un fichero log (registro) de todas las actualizaciones de las librerías.
- Se mantienen las versiones previas del software.
- En procesos que afectan a la seguridad de los sistemas de certificación, no se instala software del que el Dpto. de Ingeniería no disponga del código fuente, y haya realizado la correspondiente comprobación de seguridad en presencia de la Dirección Técnica.

6.6.2. Controles de gestión de seguridad

- ANF AC mantiene un inventario de todos los activos de información y realiza una clasificación de los mismos de acuerdo con sus necesidades de protección y coherente con el análisis de riesgos efectuado.
- Se realiza un seguimiento de las necesidades de capacidad y se planifican procedimientos para garantizar su disponibilidad.
- ANF AC monitoriza de forma continua los sistemas informáticos y comunicaciones para asegurar que operan según la Política de Seguridad de ANF AC. Todos los procesos son logueados y auditados de acuerdo con la legislación y normativa vigentes.

ANF AC mantiene los siguientes criterios con relación a la información disponible para auditorías y análisis de incidentes que pueda haber con los certificados emitidos y el tratamiento de los mismos. Los usuarios de certificados pueden comunicar a ANF AC quejas o sugerencias a través de los siguientes medios:

- Llamada telefónica: +593 02 3826877
- Correo electrónico: soporte@anf.ec
- Presencial: Av. 12 de Octubre N24-739 y Av. Colon - Ed. Torre Boreal 170143 - Quito
- Mediante la cumplimentación del formulario disponible en la web https://www.anf.ec
- Cumplimentando los formularios de quejas o reclamaciones disponibles en los puestos de registro.

Existe un registro interno de incidentes que se hayan producido con los certificados emitidos (incidentes de seguridad gestionados por el Comité de Seguridad de ANF AC). Estos incidentes se registran, analizan y solucionan según los procedimientos del SGSI de ANF AC.

En conformidad con la política de SGSI correspondiente, se actuará de manera oportuna y coordinada para responder lo antes posible a los incidentes y limitar su impacto. Se designará personal de confianza para el seguimiento de los eventos e incidentes críticos o no.

En la planificación anual de auditorías se audita específicamente la operativa de emisión de los certificados con una muestra mínima del 2% de los certificados emitidos.

En la DPC se define el periodo de conservación de la documentación.

6.6.3. Controles de seguridad del ciclo de vida

ANF AC realiza controles para proporcionar seguridad al dispositivo que realiza la generación de las claves. Para evitar posibles incidencias en los sistemas, se establecen los siguientes controles:

- El software/hardware de generación de claves es probado antes de su puesta a producción.
- La generación de claves se produce dentro de los módulos criptográficos que cumplen los requisitos de la técnica y de negocios.
- Los procedimientos para el almacenamiento seguro del hardware criptográfico y los materiales de activación se producen después de la ceremonia de generación de claves.

Los productos utilizados para la emisión de certificados disponen del certificado internacional "Common Criteria" o estándar ISO/IEC 15408:1999, o equivalente. Se procederá a la sustitución de estos productos en caso de pérdida de la certificación.

Los certificados generados en los procesos de desarrollo o pruebas, dado que no han sido puestos en producción, podrán ser desechados sin necesidad de realizar revocación, notificación a terceros ni activación del Plan de Continuidad de Negocio y Recuperación de Desastres.

6.7. Controles de seguridad de red

ANF AC opera en conformidad con las Guías de Seguridad de red de CAB Forum.

El acceso a las diferentes redes de ANF AC está limitado a personal debidamente autorizado. En particular:

- Se implementan controles para proteger la red interna de dominios externos accesibles por terceras partes. Los cortafuegos están configurados de forma que se impiden accesos y protocolos que no sean necesarios para las operaciones de servicio.
- Los datos sensibles son cifrados cuando se intercambian a través de redes no seguras (incluyendo como tales los datos de registro del suscriptor).
- Se garantiza que los componentes locales de red están ubicados en entornos seguros, así como la auditoría periódica de sus configuraciones.
- Se emplean canales de comunicación VPN, y la información confidencial que se transfiere por redes no seguras se realiza de forma cifrada mediante uso de protocolos SSL/TLS.

6.8. Time-stamping

ANF AC obtiene el tiempo de sus sistemas de una conexión al Real Observatorio de la Armada siguiendo el protocolo NTP. La descripción del protocolo NTP v.3., se puede encontrar en el estándar de IETF RFC 1305. Basándose en este servicio, ANF AC ofrece un servicio de sellado de tiempo electrónico (TSA) que puede ser utilizado para crear sellos de tiempo en documentos, según IETF RFC 3161 actualizada por IETF RFC 5816 y ETSI EN 319 421. Más información en la Política de Autoridad de Sellado de Tiempo y Declaración de Prácticas.

Para efectos legales el servicio de sellado de tiempo se prestará tomando como referencia el huso horario del territorio continental ecuatoriano UTC ("Universal Time Coordinated").

7. PERFILES DE CERTIFICADO, CRL Y OCSP

7.1. Perfil de certificado

Los certificados emitidos por ANF AC son conformes a las siguientes normas técnicas:

- Internet X.509 Public Key Infrastructure Certificate and CRL Profile (RFC 5280 (actualizada por RFC 6818)) abril 2002
- Internet X.509 Public Key Infrastructure Authority Information Access Certificate Revocation List (CRL) Extension (RFC 5280) diciembre 2005
- Update to DirectoryString Processing in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile (RFC 5280) agosto 2006
- ITU-T Recommendation X.509 (2005): Information Technology – Open Systems Interconnection – The Directory: Authentication Framework
- ETSI EN 319 412: Electronic Signatures and Infrastructures (ESI); Certificate Profiles
- RFC 3739: Internet X.509 Public Key Infrastructure – Qualified Certificate Profile

El perfil común a todos los certificados es el siguiente:

Campo	Nombre	Descripción
Versión	Nº de versión	V3 (versión del estándar X509)
Serial	nº de serie	Número no secuencial mayor que cero (0) que contiene al menos 64 bits de output de un CSPRNG.
Issuer	Emisor	DN de la CA emisora del certificado
notBefore	Válido desde	Fecha de inicio de validez, tiempo UTC
notAfter	Válido hasta	Fecha de fin de validez, tiempo UTC
Subject	Asunto (DN)	DN del suscriptor
Extensions	Extensiones	Extensiones de los certificados.

7.1.1. Número(s) de versión

Los certificados electrónicos emitidos bajo la presente Declaración de Prácticas de Certificación utilizan el estándar X.509 versión 3.

7.1.2. Extensiones del certificado

ANF AC aplica la estructura de cada tipo de certificado, según los Anexos de la Resolución ARCOTEL-2024-0176, de 16 de agosto de 2024:

1. Certificados de Persona Natural:

a) Certificado de Personas Naturales - En archivo Anexo 1a

b) Certificado de Personas Naturales - En DSCF Anexo 1b

2. Certificado de Miembro de Empresa o Empleado con Relación de dependencia:

   a) Certificado de Miembro de Empresa/ Empleado con Relación de Dependencia - En archivo Anexo 2ª

   b) Certificado de Miembro de Empresa/ Empleado con Relación de Dependencia - En DSCF Anexo 2b

3. Certificado de Representante Legal:

   a) Certificado de Representante Legal - En archivo Anexo 3a

   b) Certificado de Representante Legal - En DSCF Anexo 3b

4. Certificado de Sello Electrónico:

   a) Certificado de Sello Electrónico - En archivo Anexo 4a

   b) Certificado de Sello Electrónico- En DSCF Anexo 4b

5) Certificado de Sellado de Tiempo - Anexo 5

6) Certificado de Autoridad de Certificación Raíz (ROOT) - Anexo 6

7) Certificado de Autoridad de Certificación Subordinada - Anexo 7

8) Certificado de Validación OCSP - Anexo 8

7.1.2.1. **Certificado CA Raíz**

CERTIFICADO RAÍZ - AC (ROOT)				
Campo	**Contenido**	**Obligatorio**	**Crít.**	**Observaciones OID 1.3.6.1.4.1.OID_Ac.n**
1. Basic estructure				
1.1 Version	V3	Sí		Versión 3.
1.2 Serial Number	997415897105898611376721711	Sí		No puede ser un número negativo ni 0.
1.3 Signature Algorithm		Sí		
1.3.1 Identifier	1.2.840.113549.1.1.11	Sí		1.2.840.113549.1.1.11
1.3.2 Description	SHA-256 with RSA Signature	Sí		
1.4 **Issuer**		Sí		
1.4.1 Common Name (CN)	ANF AC Ecuador Root CA	Sí		OID 2.5.4.3

1.4.2 Country (C)	EC	Sí		OID 2.5.4.6
1.4.3 Organization Name (O)	ANFAC AUTORIDAD DE CERTIFICACION ECUADOR C.A.	Sí		OID 2.5.4.10
1.4.4 Locality (L)	QUITO	Si		OID 2.5.4.7
1.4.5 Organizational Unit (OU)	No aplica	No		OID 2.5.4.11
1.4.6 Organization Identifier	VATEC-1792601215001	No		OID 2.5.4.97 codificación acorde la ETSI EN 319 412-1 RFC 5280 establece como no obligatorio
1.5 Validity		Sí		
1.5.1 Not Before	09/10/2024	Sí		YYMMDDHHMMSSZ
1.5.2 Not After	04/10/2044	Sí		YYMMDDHHMMSSZ
1.6 Subject	**Mismos Datos entre Issuer y Subject (AutoFirmado)**	Sí		
1.6.1 Common Name (CN)	ANF AC Ecuador Root CA	Sí		OID 2.5.4.3
1.6.2 Country (C)	EC	Sí		OID 2.5.4.6
1.6.3 Organization Name(O)	ANFAC AUTORIDAD DE CERTIFICACION ECUADOR C.A.	Sí		OID 2.5.4.10
1.6.4 Locality (L)	QUITO	Sí		OID 2.5.4.7
1.6.5 Organizational Unit (OU)	No aplica	No		OID 2.5.4.11
1.6.6 organizationIdentifier	VATEC-1792601215001	No		OID 2.5.4.97 codificación acorde la ETSI EN 319 412-1 RFC 5280 establece como no obligatorio
1.7 Subject Public Key Info	**Clave pública de la AC Raíz, codificada de acuerdo con el algoritmo criptográfico.**	Sí		
1.7.1 AlgorithmIdentifier	1.2.840.113549.1.1.1			
1.7.1.1 Algorithm	RSA encryption	Sí		OID 1.2.840.113549.1.1.1
1.7.1.2 Parameters	No aplicable	No		
1.7.2 SubjectPublicKey	Clave pública codificada de acuerdo con el algoritmo criptográfico. 4096 bits	Sí		
2 Extensions				
2.1 Authority Key Identifier	Presente	No	No	OID 2.5.29.35 (Marcado como NO crítico según EN 319412-2) No es obligatorio siempre y cuando la clave pública de la AC se distribuya en forma de certificado "AUTOFIRMADO"

2.1.1 Key Identifier	Identificador de la clave del issuer	No		Derivado de la clave pública
2.2 Subject Key Identifier	Presente	Sí	No	OID 2.5.29.14 (Marcado como NO crítico según EN 319412-2)
2.2.1 KeyIdentifier	Identificador de la clave del subject	Sí		
2.3 Key Usage		Sí		OID 2.5.29.15
2.3.1 Digital Signature	No seleccionado. "0"			
2.3.2 Content commintment	No seleccionado. "0"			
2.3.3 Key Encipherment	No seleccionado. "0"			
2.3.4 Data Encipherment	No seleccionado. "0"			
2.3.5 Key Agreement	No seleccionado. "0"			
2.3.6 Key Certificate Signature	Seleccionado. "1"	Sí		
2.3.7 CRL Signature	Seleccionado. "1"	Sí		
2.4 Certificate Policies	Políticas de certificación / DPC	Sí	No	OID 2.5.29.32 (Marcado como NO crítico según EN 319412-2)
2.4.1 Policy Information		Sí		
2.4.1.1 Policy Identifier	2.5.29.32.0	Sí		Identificador de la política
2.4.1.2 Policy Qualifier ID	Especificación de la DPC	Sí		
2.4.1.2.1 CPS Pointer	https://anf.ec	Sí		
2.4.1.2.2 User Notice	https://anf.ec	Sí		
2.5 Subject Alternative Names			No	
2.5.1 rfc822Name	soporte.ec@anf.ac	Sí		
2.6 Basic Constraints		Sí	Sí	OID 2.5.29.19
2.6.1 Subject type	cA (TRUE)	Sí		
2.6.2 Path Length Constraints	0	Sí		

7.1.2.2. Certificado CA Intermedia

CERTIFICADO SUBORDINADO - AC SUB				
Campo	**Contenido**	**Obligatorio**	**Crit.**	**Observaciones OID 1.3.6.1.4.1.OID_Ac.n**
1. Basic estructure				
1.1 Version	V3	Sí		Versión 3. X.509 v3
1.2 Serial Number	Establecido automáticamente por la AC. Número identificativo único del certificado.	Sí		No puede ser un número negativo ni 0.
1.3 Signature Algorithm		Sí		
1.3.1 Identifier	1.2.840.113549.1.1.11	Sí		1.2.840.113549.1.1.11
1.3.2 Description	SHA-256 with RSA Signature	Sí		
1.4 **Issuer**		Sí		
1.4.1 Common Name (CN)	ANF AC Ecuador Root CA	Sí		OID 2.5.4.3
1.4.2 Country Name (C)	EC	Sí		OID 2.5.4.6
1.4.3 Organization Name (O)	ANFAC AUTORIDAD DE CERTIFICACION ECUADOR C.A.	Sí		OID 2.5.4.10
1.4.4 Locality Name(L)	QUITO	Si		OID 2.5.4.7
1.4.5 Organizational Unit (OU)	No aplica	No		OID 2.5.4.11
1.4.6 organizationIdentifier	VATEC-1792601215001	No		OID 2.5.4.97 codificación acorde la ETSI EN 319 412-1 RFC 5280 establece como no obligatorio
1.5 Validity		Sí		
1.5.1 Not Before	14/05/2025	Sí		YYMMDDHHMMSSZ
1.5.2 Not After	03/10/2044	Sí		YYMMDDHHMMSSZ
1.6 Subject		Sí		
1.6.1 Common Name (CN)	ANF AC Ecuador Intermediate CA	Sí		OID 2.5.4.3
1.6.2 Country Name(C)	EC	Sí		OID 2.5.4.6
1.6.3 Organization Name (O)	ANFAC AUTORIDAD DE CERTIFICACION ECUADOR C.A.	Sí		OID 2.5.4.10
1.6.4 Locality Name (L)	QUITO	Sí		OID 2.5.4.7
1.6.5 Organizational Unit (OU)	No aplica	No		OID 2.5.4.11

1.6.6 Organization Identifier	VATEC-1792601215001	No		OID 2.5.4.97 codificación acorde la ETSI EN 319 412-1 RFC 5280 establece como no obligatorio
1.7 Subject Public Key Info	Clave pública del prestador, codificada de acuerdo con el algoritmo criptográfico.	Sí		
1.7.1 AlgorithmIdentifier	1.2.840.113549.1.1.1			OID 1.2.840.113549.1.1.1
1.7.1.1 Algorithm	RSA encryption	Sí		
1.7.1.2 Parameters	No aplicable	No		
1.7.2 SubjectPublicKey	Clave pública codificada de acuerdo con el algoritmo criptográfico. 4096 bits	Sí		
2 Extensions				
2.1 Authority Key Identifier	Presente	No	No	OID 2.5.29.35 (Marcado como NO crítico según EN 319412-2) No es obligatorio siempre y cuando la clave pública de la AC se distribuya en forma de certificado "AUTOFIRMADO"
2.1.1 Key Identifier	Identificador de la clave del Issuer	No		
2.2 Subject Key Identifier	Presente	Sí	No	OID 2.5.29.14 (Marcado como NO crítico según EN 319412-2)
2.2.1 KeyIdentifier	Identificador de la clave del subject	Sí		
2.3 Key Usage		Sí		OID 2.5.29.15
2.3.1 Digital Signature	No seleccionado. "0"			
2.3.2 Content commintment	No seleccionado. "0"			
2.3.3 Key Encipherment	No seleccionado. "0"			
2.3.4 Data Encipherment	No seleccionado. "0"			
2.3.5 Key Agreement	No seleccionado. "0"			
2.3.6 Key Certificate Signature	Seleccionado. "1"	Sí		
2.3.7 CRL Signature	Seleccionado. "1"	Sí		
2.4 Certificate Policies	Políticas de certificación / DPC	Sí	No	OID 2.5.29.32 (Marcado como NO crítico según EN 319412-2)
2.4.1 Policy Information		Sí		
2.4.1.1 Policy Identifier	2.5.29.32.0	Sí		Identificador de la política

2.4.1.2 Policy Qualifier ID	Especificación de la DPC	Sí		
2.4.1.2.1 CPS Pointer	https://anf.ec	Sí		
2.4.1.2.2 User Notice	https://anf.ec	Sí		
2.5 Subject Alternative Names		No	No	OID 2.5.29.17 (Marcado como NO crítico según EN 319412-2)
2.5.1 rfc822Name	soporte.ec@anf.ac	Sí		
2.6 cRLDistributionPoint		Sí		OID 2.5.29.31 (Marcado como NO crítico según EN 319412-2)
2.6.1 distributionPoint	http://crl.anf.es/crl/ANFACEcuadorRootCA.crl	Sí		http (http://) IETF RFC 7230-7235 [3] or ldap (ldap://) IETF RFC 4516 [4] scheme
2.6.2 distributionPoint	No aplica	No		http (http://) IETF RFC 7230-7235 [3] or ldap (ldap://) IETF RFC 4516 [4] scheme
2.7 Authority Information Access		No	No	OID 1.3.6.1.5.5.7.1.1 (Marcado como NO crítico según EN 319412-2)
2.7.1 Access Method	id-ad-ocsp	No		OID 1.3.6.1.5.5.7.48.1
2.7.2 Access Location	http://ocsp.anf.es/spain/AV	No		URL de acceso al OCSP (http://) IETF RFC 7230-7235 [3] or https (https://) IETF RFC 2818 [5]
2.7.3 Access Location	No aplica	No		URL de acceso al OCSP (http://) IETF RFC 7230-7235 [3] or https (https://) IETF RFC 2818 [5]
2.8 Basic Constraints		Sí	Sí	OID 2.5.29.19
2.8.1 Subject type	cA (TRUE)	Sí		
2.8.2 Path Length Constraints	0	Sí		

7.1.2.3. Certificados de usuario final

PERSONA NATURAL EN ARCHIVO				
Campo	**en Archivo**	**Oblig.**	**Crít.**	**Observaciones OID 1.3.6.1.4.1.37442.2.1.1**
De Persona Natural	**Autenticación y Firma**			
1. Basic estructure				
1.1. Version	V3	Sí		Versión 3. X.509 v3
1.2. Serial Number	Establecido automáticamente por la AC Número identificativo único del certificado.	Sí		No puede ser un número negativo ni 0.
1.3. Signature Algorithm		Sí		
1.3.1. Algorithm	SHA-256 with RSA Signature	Sí		1.2.840.113549.1.1.11
1.3.2. Parameters	No aplicable	No		
1.4. Issuer		Sí		
1.4.1. Country Name (C)	EC	Sí		OID 2.5.4.6
1.4.2. Organization Name(O)	ANFAC AUTORIDAD DE CERTIFICACION ECUADOR C.A.	Sí		OID 2.5.4.10
1.4.3. Locality Name (L)	QUITO	Sí		OID 2.5.4.7
1.4.4. Organization Identifier	VATEC-1792601215001	No		OID 2.5.4.97 codificación acorde la ETSI EN 319 412-1 RFC 5280 establece como no obligatorio
1.4.5. Common Name (CN)	ANF AC Ecuador Intermediate CA	Sí		OID 2.5.4.3
1.4.6. Organizational Unit Name (OU)	No aplica	No		OID 2.5.4.11
1.5. Validity		Sí		
1.5.1. Not Before	Fecha de inicio de validez	Sí		YYMMDDHHMMSSZ
1.5.2. Not After	Fecha de expiración	Sí		YYMMDDHHMMSSZ
1.6. Subject		Sí		
1.6.1. Country Name (C)	País donde reside el Titular de la Firma "EC" (ISO 3166)	Sí		OID 2.5.4.6
1.6.2. Locality Name (L)	Localidad del Titular de la Firma (Ciudad) ej. QUITO	Sí		OID 2.5.4.7
1.6.3. Title	Título o especialidad del Titular de la Firma	No		OID 2.5.4.12
1.6.4. Surname	Apellidos del Titular de la Firma (como consta en el documento oficial)	Sí		OID 2.5.4.4

1.6.5. Given Name	Nombres del Titular de la firma (como consta en el documento oficial)	Sí		OID 2.5.4.42
1.6.6. Serial Number	Número de cédula (IDC"Pais"-1716151413) o pasaporte (PAS"País"-A6362611) Ej. IDCEC-1716151413 o PASEC-A6362611	Sí		OID 2.5.4.5 Número de documento oficial codificado acorde a ETSI EN 319 412-1
1.6.7. Organization Identifier	Número de Registro Unico de Contribuyente TIN(CÓDIGO_PAÍS)-RUC Ej. ("TINEC-1716151413001")	No		OID 2.5.4.97 codificación acorde la ETSI EN 319 412-1 RFC 5280 establece como no obligatorio
1.6.8. Common Name (CN)	Nombres y Apellidos del Titular de la Firma	Sí		OID 2.5.4.3
1.7. Subject Public Key Info		Sí		
1.7.1. AlgorithmIdentifier				
1.7.1.1. Algorithm	RSA encryption	Sí		OID 1.2.840.113549.1.1.1
1.7.1.2. Parameters	No aplicable	No		
1.7.2. SubjectPublicKey	Clave pública del Titular de la Firma	Sí		Acorde ETSI TS 119 312
2. Extensions				
2.1. Authority Key Identifier	Identificador de la clave del Issuer	No	No	OID 2.5.29.35 (Marcado como NO crítico según EN 319412-2) No es obligatorio siempre y cuando la clave pública de la AC se distribuya en forma de certificado "AUTOFIRMADO"
2.1.1. KeyIdentifier		No		Derivado de la clave pública
2.2. Subject Key Identifier	Identificador de la clave del Subject	Sí	No	OID 2.5.29.14 (Marcado como NO crítico según EN 319412-2)
2.2.1. KeyIdentifier		Sí		Derivado de la clave pública
2.3. Key Usage		Sí	Sí	OID 2.5.29.15
2.3.1. Digital Signature	Seleccionado "1"	Sí		
2.3.2. Content commintment	Seleccionado "1"	Sí		
2.3.3. Key Encipherment	Seleccionado "1"	Sí		
2.3.4. Data Encipherment	No seleccionado. "0"			
2.3.5. Key Agreement	No seleccionado. "0"			
2.3.6. Key Certificate Signature	No seleccionado. "0"			
2.3.7. CRL Signature	No seleccionado. "0"			

2.3.8. Encipher Only	No seleccionado. "0"			
2.3.9. Decipher Only	No seleccionado. "0"			
2.4. Certificate Policies		Si	No	OID 2.5.29.32 (Marcado como NO crítico según EN 319412-2)
2.4.1. Policy Information		Sí		
2.4.1.1. Policy Identifier	1.3.6.1.4.1.37442.2.1.1	Sí		Identificador de la política de la AC
2.4.1.2. Policy Qualifiers		Sí		
2.4.1.1.1 CPS URI	https://anf.ec	Sí		OID 1.3.6.1.5.5.7.2.1 URL de la Política de Certificados de la Entidad Acreditada
2.4.1.1.2. User Notice/Explicit text	CERTIFICADO DE PERSONA NATURAL EN ARCHIVO	Sí		OID 1.3.6.1.5.5.7.2.2 Texto indicativo
2.5. Subject Alternative Names		No	No	OID 2.5.29.17 (Marcado como NO crítico según EN 319412-2)
2.5.1. rfc822Name	Correo electrónico del Titular de la Firma "nombreapellido@example.com.ec"	Sí		
2.6. Extended Key Usage		Sí	No	OID 2.5.29.37 (Marcado como NO crítico según EN 319412-2)
2.6.1. clientAuth	Presente (1.3.6.1.5.5.7.3.2)	Sí		Transport Layer Security (TLS) World Wide Web (WWW) client authentication
2.6.2. Email protection	Presente (1.3.6.1.5.5.7.3.4)	No		Sólo se activa si se incluye el correo electrónico del Titular de la Firma
2.7.cRLDistributionPoint		No	No	OID 2.5.29.31 (Marcado como NO crítico según EN 319412-2)
2.7.1. distributionPoint	http://crl.anf.es/crl/ANFACEcuadorIntermediateCA.crl	Sí		http (http://) IETF RFC 7230-7235 [3] or ldap (ldap://) IETF RFC 4516 [4] scheme
2.7.2. distributionPoint	No aplica	No		http (http://) IETF RFC 7230-7235 [3] or ldap (ldap://) IETF RFC 4516 [4] scheme
2.8. Authority Information Access		Sí	No	OID 1.3.6.1.5.5.7.1.1 (Marcado como NO crítico según EN 319412-2)
2.8.1. Access Description		Sí		

2.8.1.1. Access Method	id-ad-ocsp	Sí		OID 1.3.6.1.5.5.7.48.1
2.8.1.1.1 Access Location	http://ocsp.anf.es/spain/AV	Sí		URL de acceso al OCSP (http://) IETF RFC 7230-7235 [3] or https (https://) IETF RFC 2818 [5]
2.8.1.1.2. Access Location	No aplica	No		URL de acceso al OCSP (http://) IETF RFC 7230-7235 [3] or https (https://) IETF RFC 2818 [5]
2.8.2. Access Description		No		No es obligatorio siempre y cuando incluya la ubicación de acceso al OCSP
2.8.2.1. Access Method	id-ad-calssuers	No		OID 1.3.6.1.5.5.7.48.2
2.8.2.1.1 Access Location	http://crl.anf.es/certificates-download/ANFACEcuadorIntermediateCA.cer	No		URL acceso a certificado de la AC (http://) IETF RFC 7230-7235 [3] or https (https://) IETF RFC 2818 [5]
2.9. Basic Constraints		Sí	Sí	OID 2.5.29.19
2.9.1. cA	FALSE	Sí		

PERSONA NATURAL EN DSCF				
Campo	**en Dispositivo Seguro de Creación de Firma "DSCF"**	**Oblig.**	**Crít.**	**Observaciones OID 1.3.6.1.4.1.37442.2.1.2**
De Persona Natural	**Autenticación y Firma**			
1. Basic estructure				
1.1. Version	V3	Sí		Versión 3. X.509 v3
1.2. Serial Number	Establecido automáticamente por la AC. Número identificativo único del certificado.	Sí		No puede ser un número negativo ni 0.
1.3. Signature Algorithm		Sí		
1.3.1. Algorithm	SHA-256 with RSA Signature	Sí		1.2.840.113549.1.1.11
1.3.2. Parameters	No aplicable	No		
1.4. Issuer		Sí		
1.4.1. Country Name (C)	EC	Sí		OID 2.5.4.6
1.4.2. Organization Name (O)	ANFAC AUTORIDAD DE CERTIFICACION ECUADOR C.A.	Sí		OID 2.5.4.10
1.4.3. Locality Name (L)	QUITO	Sí		OID 2.5.4.7

1.4.4. Organization Identifier	VATEC-1792601215001	No		OID 2.5.4.97 codificación acorde la ETSI EN 319 412-1 RFC 5280 establece como no obligatorio
1.4.5. Common Name (CN)	ANF AC Ecuador Intermediate CA	Sí		OID 2.5.4.3
1.4.6. Organizational Unit Name (OU)	No aplica	No		OID 2.5.4.11
1.5. Validity		Sí		
1.5.1. Not Before	Fecha de inicio de validez	Sí		YYMMDDHHMMSSZ
1.5.2. Not After	Fecha de expiración	Sí		YYMMDDHHMMSSZ
1.6. Subject		Sí		
1.6.1. Country Name (C)	País donde reside el Titular de la Firma "EC" (ISO 3166)	Sí		OID 2.5.4.6
1.6.2. Locality Name (L)	Localidad del Titular de la Firma (Ciudad) ej. QUITO	Sí		OID 2.5.4.7
1.6.3. Title	Título o especialidad del Titular de la Firma	No		OID 2.5.4.12
1.6.4. Surname	Apellidos del Titular de la Firma (como consta en el documento oficial)	Sí		OID 2.5.4.4
1.6.5. Given Name	Nombres del Titular de la firma (como consta en el documento oficial)	Sí		OID 2.5.4.42
1.6.6. Serial Number	Número de cédula (IDC"Pais"-1716151413) o pasaporte (PAS"País"-A6362611) Ej. IDCEC-1716151413 o PASEC-A6362611	Sí		OID 2.5.4.5 Número de documento oficial codificado acorde a ETSI EN 319 412-1
1.6.7. Organization Identifier	Número de Registro Unico de Contribuyente TIN(CÓDIGO_PAÍS)-RUC Ej. ("TINEC-1716151413001")	No		OID 2.5.4.97 codificación acorde la ETSI EN 319 412-1 RFC 5280 establece como no obligatorio
1.6.8. Common Name (CN)	Nombres y Apellidos del Titular de la Firma	Sí		OID 2.5.4.3
1.7. Subject Public Key Info		Sí		
1.7.1. AlgorithmIdentifier				
1.7.1.1. Algorithm	RSA encryption	Sí		OID 1.2.840.113549.1.1.1
1.7.1.2. Parameters	No aplicable	No		
1.7.2. SubjectPublicKey	Clave pública del Titular de la Firma	Sí		Acorde ETSI TS 119 312

2. Extensions				
2.1. Authority Key Identifier	Identificador de la clave del Issuer	No	No	OID 2.5.29.35 (Marcado como NO crítico según EN 319412-2) No es obligatorio siempre y cuando la clave pública de la AC se distribuya en forma de certificado "AUTOFIRMADO"
2.1.1. KeyIdentifier		No		Derivado de la clave pública
2.2. Subject Key Identifier	Identificador de la clave del Subject	Sí	No	OID 2.5.29.14 (Marcado como NO crítico según EN 319412-2)
2.2.1. KeyIdentifier		Sí		Derivado de la clave pública
2.3. Key Usage		Sí	Sí	OID 2.5.29.15
2.3.1. Digital Signature	Seleccionado "1"	Sí		
2.3.2. Content commintment	Seleccionado "1"	Sí		
2.3.3. Key Encipherment	Seleccionado "1"	Sí		
2.3.4. Data Encipherment	No seleccionado. "0"			
2.3.5. Key Agreement	No seleccionado. "0"			
2.3.6. Key Certificate Signature	No seleccionado. "0"			
2.3.7. CRL Signature	No seleccionado. "0"			
2.3.8. Encipher Only	No seleccionado. "0"			
2.3.9. Decipher Only	No seleccionado. "0"			
2.4. Certificate Policies		Si	No	OID 2.5.29.32 (Marcado como NO crítico según EN 319412-2)
2.4.1. Policy Information		Sí		
2.4.1.1. Policy Identifier	1.3.6.1.4.1.37442.2.1.2	Sí		Identificador de la política de la AC
2.4.1.2. Policy Qualifiers		Sí		
2.4.1.1.1 CPS URI	https://www.anf.ec	Sí		OID 1.3.6.1.5.5.7.2.1 URL de la Política de Certificados de la Entidad Acreditada

2.4.1.1.2. User Notice/Explicit text	CERTIFICADO DE PERSONA NATURAL EN DISPOSITIVO SEGURO DE CREACIÓN DE FIRMA - DSCF	Sí		OID 1.3.6.1.5.5.7.2.2 Texto indicativo
2.5. Subject Alternative Names		No	No	OID 2.5.29.17 (Marcado como NO crítico según EN 319412-2)
2.5.1. rfc822Name	Correo electrónico del Titular de la Firma "nombreapellido@example.com.ec"	Sí		
2.6. Extended Key Usage		Sí	No	OID 2.5.29.37 (Marcado como NO crítico según EN 319412-2)
2.6.1. clientAuth	Presente (1.3.6.1.5.5.7.3.2)	Sí		Transport Layer Security (TLS) World Wide Web (WWW) client authentication
2.6.2. Email protection	Presente (1.3.6.1.5.5.7.3.4)	No		Sólo se activa si se incluye el correo electrónico del Titular d ela Firma
2.7.cRLDistributionPoint		No	No	OID 2.5.29.31 (Marcado como NO crítico según EN 319412-2)
2.7.1. distributionPoint	http://crl.anf.es/crl/ANFACEcuadorIntermediateCA.crl	Sí		http (http://) IETF RFC 7230-7235 [3] or ldap (ldap://) IETF RFC 4516 [4] scheme
2.7.2. distributionPoint	No aplica	No		http (http://) IETF RFC 7230-7235 [3] or ldap (ldap://) IETF RFC 4516 [4] scheme
2.8. Authority Information Access		Sí	No	OID 1.3.6.1.5.5.7.1.1 (Marcado como NO crítico según EN 319412-2)
2.8.1. Access Description		Sí		
2.8.1.1. Access Method	id-ad-ocsp	Sí		OID 1.3.6.1.5.5.7.48.1
2.8.1.1.1 Access Location	http://ocsp.anf.es/spain/AV	Sí		URL de acceso al OCSP (http://) IETF RFC 7230-7235 [3] or https (https://) IETF RFC 2818 [5]
2.8.1.1.2. Access Location	No aplica	No		URL de acceso al OCSP (http://) IETF RFC 7230-7235 [3] or https (https://) IETF RFC 2818 [5]

2.8.2. Access Description		No		No es obligatorio siempre y cuando incluya la ubicación de acceso al OCSP
2.8.2.1. Access Method	id-ad-calssuers	No		OID 1.3.6.1.5.5.7.48.2
2.8.2.1.1 Access Location	http://crl.anf.es/certificates-download/ANFACEcuadorIntermediateCA.cer	No		URL acceso a certificado de la CA (http://) IETF RFC 7230-7235 [3] or https (https://)IETF RFC 2818 [5]
2.9. Basic Constraints		Sí	Sí	OID 2.5.29.19
2.9.1. cA	FALSE	Sí		

MIEMBRO DE EMPRESA O EMPLEADO CON RELACIÓN DE DEPENDENCIA EN ARCHIVO				
Campo	**en Archivo**	**Oblig.**	**Crít.**	**Observaciones OID 1.3.6.1.4.1.37442.2.2.1**
De Miembro de Empresa o Relación de Dependencia	**Autenticación y Firma**			
1. Basic estructure				
1.1. Version	V3	Sí		Versión 3. X.509 v3
1.2. Serial Number	Establecido automáticamente por la AC. Número identificativo único del certificado.	Sí		No puede ser un número negativo ni 0.
1.3. Signature Algorithm		Sí		
1.3.1. Algorithm	SHA-256 with RSA Signature	Sí		1.2.840.113549.1.1.11
1.3.2. Parameters	No aplicable	No		
1.4. Issuer		Sí		
1.4.1. Country Name (C)	EC	Sí		OID 2.5.4.6
1.4.2. Organization Name (O)	ANFAC AUTORIDAD DE CERTIFICACION ECUADOR C.A.	Sí		OID 2.5.4.10
1.4.3. Locality Name (L)	QUITO	Sí		OID 2.5.4.7
1.4.4. Organization Identifier	VATEC-1792601215001	No		OID 2.5.4.97 codificación acorde la ETSI EN 319 412-1 RFC 5280 establece como no obligatorio
1.4.5. Common Name (CN)	ANF AC Ecuador Intermediate CA	Sí		OID 2.5.4.3

1.4.6.Organizational Unit (OU)	No aplica	No		OID 2.5.4.11
1.5. Validity		Sí		
1.5.1. Not Before	Fecha de inicio de validez	Sí		YYMMDDHHMMSSZ
1.5.2. Not After	Fecha de expiración	Sí		YYMMDDHHMMSSZ
1.6. Subject		Sí		
1.6.1. Country Name (C)	País donde reside el Signatario "EC" (ISO 3166)	Sí		OID 2.5.4.6
1.6.2. Locality Name (L)	Localidad del Signatario (Ciudad) ej. QUITO	Sí		OID 2.5.4.7
1.6.3. Organization Name (O)	Se especificará el nombre de la Persona Natural o Persona Jurídica (Pública o Privada) a la que pertenece el Signatario o con quien tiene relación de dependencia. Ej. CORPORACION FAVORITA	Sí		OID 2.5.4.10
1.6.4. Organizational Unit Name (OU)	Se especificará el Departamento o Área al que pertenece el Signatario o el tipo de vinculación con la Persona Natural o Persona Jurídica (Pública o Privada) que tiene relación de dependencia.	No		OID 2.5.4.11
1.6.5. Organization Identifier	Número de Registro Unico de Contribuyente de la persona jurídica (Pública o Privada) a la que está vinculado el Signatario "VAT(CÓDIGO_PAÍS)-RUC". Ej. VATEC-1716151413001	No		OID 2.5.4.97 codificación acorde la ETSI EN 319 412-1 RFC 5280 establece como no obligatorio
1.6.6. Title	Se especificará el nombre del título o el puesto (cargo) que el Signatario ocupa	Sí		OID 2.5.4.12
1.6.7. Surname	Apellidos del Signatario (como consta en el documento oficial)	Sí		OID 2.5.4.4
1.6.8. Given Name	Nombres del Signatario (como consta en el documento oficial)	Sí		OID 2.5.4.42
1.6.9. Serial Number	Número de cédula (IDC"Pais"-1716151413) o pasaporte (PAS"País"-A6362611) del Signatario. Ej. IDCEC-1716151413 o PASEC-A6362611	Sí		OID 2.5.4.5 Número de documento oficial codificado acorde a ETSI EN 319 412-1
1.6.10. Common Name	Nombres y Apellidos del Signatario	Sí		OID 2.5.4.3
1.7. Subject Public Key Info		Sí		
1.7.1.AlgorithmIdentifier				
1.7.1.1. Algorithm	RSA encryption	Sí		OID 1.2.840.113549.1.1.1

1.7.1.2. Parameters	No aplicable	No		
1.7.2.SubjectPublic Key	Clave pública del Signatario	Sí		Acorde ETSI TS 119 312
2. Extensions				
2.1. Authority Key Identifier	Identificador de la clave del Issuer	No	No	OID 2.5.29.35 (Marcado como NO crítico según EN 319412-2) No es obligatorio siempre y cuando la clave pública de la AC se distribuya en forma de certificado "AUTOFIRMADO"
2.1.1. KeyIdentifier		No		Derivado de la clave pública
2.2. Subject Key Identifier	Identificador de la clave del Subject	Sí	No	OID 2.5.29.14 (Marcado como NO crítico según EN 319412-2)
2.2.1. KeyIdentifier		Sí		Derivado de la clave pública
2.3. Key Usage		Sí	Sí	OID 2.5.29.15
2.3.1. Digital Signature	Seleccionado "1"	Sí		
2.3.2. Content commintment	Seleccionado "1"	Sí		
2.3.3. Key Enciphermen t	Seleccionado "1"	Sí		
2.3.4. Data Enciphermen t	No seleccionado. "0"			
2.3.5. Key Agreement	No seleccionado. "0"			
2.3.6. Key Certificate Signature	No seleccionado. "0"			
2.3.7. CRL Signature	No seleccionado. "0"			
2.3.8. Encipher Only	No seleccionado. "0"			
2.3.9. Decipher Only	No seleccionado. "0"			
2.4. Certificate Policies		Si	No	OID 2.5.29.32 (Marcado como NO crítico según EN 319412-2)
2.4.1. Policy Information		Sí		
2.4.1.1. Policy Identifier	1.3.6.1.4.1.37442.2.2.11	Sí		Identificador de la política de la AC

2.4.1.2. Policy Qualifiers		Sí		
2.4.1.1.1 CPS URI	https://www.anf.ec	Sí		OID 1.3.6.1.5.5.7.2.1 URL de la Política de Certificados de la Entidad Acreditada
2.4.1.1.2. User Notice/Explicit text	CERTIFICADO DE MIEMBRO DE EMPRESA O EN RELACION DE DEPENDENCIA EN ARCHIVO	Sí		OID 1.3.6.1.5.5.7.2.2 Texto indicativo
2.5. Subject Alternative Names		No	No	OID 2.5.29.17 (Marcado como NO crítico según EN 319412-2)
2.5.1. rfc822Name	Correo electrónico del Signatario "nombreapellido@example.com.ec"	Sí		
2.6. Extended Key Usage		Sí	No	OID 2.5.29.37 (Marcado como NO crítico según EN 319412-2)
2.6.1. clientAuth	Presente (1.3.6.1.5.5.7.3.2)	Sí		Transport Layer Security (TLS) World Wide Web (WWW) client authentication
2.6.2. Email protection	Presente (1.3.6.1.5.5.7.3.4)	No		Sólo se activa si se incluye el correo electrónico del Signatario
2.7. cRLDistribution Point		No	No	OID 2.5.29.31 (Marcado como NO crítico según EN 319412-2)
2.7.1. distributionPoint	http://crl.anf.es/crl/ANFACEcuadorIntermediateCA.crl	Sí		http (http://) IETF RFC 7230-7235 [3] or ldap (ldap://) IETF RFC 4516 [4] scheme
2.7.2. distributionPoint	No aplica	No		http (http://) IETF RFC 7230-7235 [3] or ldap (ldap://) IETF RFC 4516 [4] scheme
2.8. Authority Information Access		Sí	No	OID 1.3.6.1.5.5.7.1.1 (Marcado como NO crítico según EN 319412-2)
2.8.1. Access Description		Sí		
2.8.1.1. Access Method	id-ad-ocsp	Sí		OID 1.3.6.1.5.5.7.48.1
2.8.1.1.1 Access Location	http://ocsp.anf.es/spain/AV	Sí		URL de acceso al OCSP (http://) IETF RFC 7230-7235 [3] or https (https://) IETF RFC 2818 [5]

2.8.1.1.2. Access Location	No aplica	No		URL de acceso al OCSP (http://) IETF RFC 7230-7235 [3] or https (https://) IETF RFC 2818 [5]
2.8.2. Access Description		No		No es obligatorio siempre y cuando incluya la ubicación de acceso al OCSP
2.8.2.1. Access Method	id-ad-calssuers	No		OID 1.3.6.1.5.5.7.48.2
2.8.2.1.1 Access Location	http://crl.anf.es/certificates-download/ANFACEcuadorIntermediateCA.cer	No		URL acceso a certificado de la CA (http://) IETF RFC 7230-7235 [3] or https (https://) IETF RFC 2818 [5]
2.9. Basic Constraints		Sí	Sí	OID 2.5.29.19
2.9.1. cA	FALSE	Sí		

MIEMBRO DE EMPRESA O EMPLEADO CON RELACIÓN DE DEPENDENCIA EN DSCF				
Campo	**en Dispositivo Seguro de Creación de Firma DSCF**	**Oblig.**	**Crít.**	**Observaciones OID 1.3.6.1.4.1.37442.2.2.2**
De Miembro de Empresa o Relación de Dependencia	**Autenticación y Firma**			
1. Basic estructure				
1.1. Version	V3	Sí		Versión 3. X.509 v3
1.2. Serial Number	Establecido automáticamente por la CA. Número identificativo único del certificado.	Sí		No puede ser un número negativo ni 0.
1.3. Signature Algorithm		Sí		
1.3.1. Algorithm	SHA-256 with RSA Signature	Sí		1.2.840.113549.1.1.11
1.3.2. Parameters	No aplicable	No		
1.4. Issuer		Sí		
1.4.1. Country Name (C)	EC	Sí		OID 2.5.4.6
1.4.2. Organization Name (O)	ANFAC AUTORIDAD DE CERTIFICACION ECUADOR C.A.	Sí		OID 2.5.4.10
1.4.3. Locality Name (L)	QUITO	Sí		OID 2.5.4.7

1.4.4. Organization Identifier	VATEC-1792601215001	No		OID 2.5.4.97 codificación acorde la ETSI EN 319 412-1 RFC 5280 establece como no obligatorio
1.4.5. Common Name (CN)	ANF AC Ecuador Intermediate CA	Sí		OID 2.5.4.3
1.4.6. Organizational Unit (OU)	No aplica	No		OID 2.5.4.11
1.5. Validity		Sí		
1.5.1. Not Before	Fecha de inicio de validez	Sí		YYMMDDHHMMSSZ
1.5.2. Not After	Fecha de expiración	Sí		YYMMDDHHMMSSZ
1.6. Subject		Sí		
1.6.1. Country Name (C)	País donde reside el Signatario "EC" (ISO 3166)	Sí		OID 2.5.4.6
1.6.2. Locality Name (L)	Localidad del Signatario (Ciudad) ej. QUITO	Sí		OID 2.5.4.7
1.6.3. Organization Name (O)	Se especificará el nombre de la Persona Natural o Persona Jurídica (Pública o Privada) a la que pertenece el Signatario o con quien tiene relación de dependencia. Ej. CORPORACION FAVORITA	Sí		OID 2.5.4.10
1.6.4. Organizational Unit Name (OU)	Se especificará el Departamento o Área al que pertenece el Signatario o el tipo de vinculación con la Persona Natural o Persona Jurídica (Pública o Privada) que tiene relación de dependencia.	No		OID 2.5.4.11
1.6.5. Organization Identifier	Número de Registro Unico de Contribuyente de la persona jurídica (Pública o Privada) a la que está vinculado el Signatario "VAT(CÓDIGO_PAÍS)-RUC" Ej. VATEC-1716151413001	No		OID 2.5.4.97 codificación acorde la ETSI EN 319 412-1 RFC 5280 establece como no obligatorio
1.6.6. Title	Se especificará el nombre del título o el puesto (cargo) que el Signatario ocupa	Sí		OID 2.5.4.12
1.6.7. Surname	Apellidos del Signatario (como consta en el documento oficial)	Sí		OID 2.5.4.4
1.6.8. Given Name	Nombres del Signatario (como consta en el documento oficial)	Sí		OID 2.5.4.42
1.6.9. Serial Number	Número de cédula (IDC"Pais"-1716151413) o pasaporte (PAS"País"-A6362611) del Signatario Ej. IDCEC-1716151413 o PASEC-A6362611	Sí		OID 2.5.4.5 Número de documento oficial codificado acorde a ETSI EN 319 412-1
1.6.10. Common Name	Nombres y Apellidos del Signatario	Sí		OID 2.5.4.3
1.7. Subject Public Key Info		Sí		

1.7.1. AlgorithmIdentifier				
1.7.1.1. Algorithm	RSA encryption	Sí		OID 1.2.840.113549.1.1.1
1.7.1.2. Parameters	No aplicable	No		
1.7.2. SubjectPublicKey	Clave pública del Signatario	Sí		Acorde ETSI TS 119 312
2. Extensions				
2.1. Authority Key Identifier	Identificador de la clave del Issuer	No	No	OID 2.5.29.35 (Marcado como NO crítico según EN 319412-2) No es obligatorio siempre y cuando la clave pública de la AC se distribuya en forma de certificado "AUTOFIRMADO"
2.1.1. KeyIdentifier		No		Derivado de la clave pública
2.2. Subject Key Identifier	Identificador de la clave del Subject	Sí	No	OID 2.5.29.14 (Marcado como NO crítico según EN 319412-2)
2.2.1. KeyIdentifier		Sí		Derivado de la clave pública
2.3. Key Usage		Sí	Sí	OID 2.5.29.15
2.3.1. Digital Signature	Seleccionado "1"	Sí		
2.3.2. Content commintment	Seleccionado "1"	Sí		
2.3.3. Key Encipherment	Seleccionado "1"	Sí		
2.3.4. Data Encipherment	No seleccionado. "0"			
2.3.5. Key Agreement	No seleccionado. "0"			
2.3.6. Key Certificate Signature	No seleccionado. "0"			
2.3.7. CRL Signature	No seleccionado. "0"			
2.3.8. Encipher Only	No seleccionado. "0"			
2.3.9. Decipher Only	No seleccionado. "0"			
2.4. Certificate Policies		Si	No	OID 2.5.29.32 (Marcado como NO crítico según EN 319412-2)
2.4.1. Policy Information		Sí		

2.4.1.1. Policy Identifier	1.3.6.1.4.1.37442.2.2.2	Sí		Identificador de la política de la AC
2.4.1.2. Policy Qualifiers		Sí		
2.4.1.1.2. User Notice/Explicit text	CERTIFICADO DE MIEMBRO DE EMPRESA O EN RELACION DE DEPENDENCIA EN DISPOSITIVO SEGURO DE CREACIÓN DE FIRMA - DSCF	Sí		OID 1.3.6.1.5.5.7.2.2 Texto indicativo
2.5. Subject Alternative Names		**Sí**		
2.5.1. rfc822Name	Correo electrónico del Signatario "nombreapellido@example.com.ec"	Sí		
2.6. Extended Key Usage		Sí	No	OID 2.5.29.37 (Marcado como NO crítico según EN 319412-2)
2.6.1. clientAuth	Presente (1.3.6.1.5.5.7.3.2)	Sí		Transport Layer Security (TLS) World Wide Web (WWW) client authentication
2.6.2. Email protection	Presente (1.3.6.1.5.5.7.3.4)	No		Sólo se activa si se incluye el correo electrónico del Signatario
2.7.cRLDistributionPoint		No	No	OID 2.5.29.31 (Marcado como NO crítico según EN 319412-2)
2.7.1. distributionPoint	http://crl.anf.es/crl/ANFACEcuadorIntermediateCA.crl	Sí		http (http://) IETF RFC 7230-7235 [3] or ldap (ldap://) IETF RFC 4516 [4] scheme
2.7.2. distributionPoint	No aplica	No		http (http://) IETF RFC 7230-7235 [3] or ldap (ldap://) IETF RFC 4516 [4] scheme
2.8. Authority Information Access		Sí	No	OID 1.3.6.1.5.5.7.1.1 (Marcado como NO crítico según EN 319412-2)
2.8.1. Access Description		Sí		
2.8.1.1. Access Method	id-ad-ocsp	Sí		OID 1.3.6.1.5.5.7.48.1
2.8.1.1.1 Access Location	http://ocsp.anf.es/spain/AV	Sí		http (http://) IETF RFC 7230-7235 [3] or ldap (ldap://) IETF RFC 4516 [4] scheme
2.8.1.1.2. Access Location	No aplica	No		http (http://) IETF RFC 7230-7235 [3] or ldap (ldap://) IETF RFC 4516 [4] scheme

2.8.2. Access Description		No		No es obligatorio siempre y cuando incluya la ubicación de acceso al OCSP
2.8.2.1. Access Method	id-ad-calssuers	No		OID 1.3.6.1.5.5.7.48.2
2.8.2.1.1 Access Location	http://crl.anf.es/certificates-download/ANFACEcuadorIntermediateCA.cer	No		URL acceso a certificado de la CA (http://) IETF RFC 7230-7235 [3] or https (https://) IETF RFC 2818 [5]
2.9. Basic Constraints		Sí	Sí	OID 2.5.29.19
2.9.1. cA	FALSE	Sí		

REPRESENTANTE LEGAL EN ARCHIVO				
Campo	**en Archivo**	**Oblig.**	**Crít.**	**Observaciones OID 1.3.6.1.4.1.37442.2.3.1**
De Representante Legal	**Autenticación y Firma**			
1. Basic estructure				
1.1. Version	V3	Sí		Versión 3. X.509 v3
1.2. Serial Number	Establecido automáticamente por la AC. Número identificativo único del certificado.	Sí		No puede ser un número negativo ni 0.
1.3. Signature Algorithm		Sí		
1.3.1. Algorithm	SHA-256 with RSA Signature	Sí		1.2.840.113549.1.1.11
1.3.2. Parameters	No aplicable	No		
1.4. Issuer		Sí		
1.4.1. Country Name (C)	EC	Sí		OID 2.5.4.6
1.4.2. Organization Name (O)	ANFAC AUTORIDAD DE CERTIFICACION ECUADOR C.A.	Sí		OID 2.5.4.10
1.4.3. Locality Name (L)	QUITO	Sí		OID 2.5.4.7
1.4.4. Organization Identifier	VATEC-1792601215001	No		OID 2.5.4.97 codificación acorde la ETSI EN 319 412-1 RFC 5280 establece como no obligatorio
1.4.5. Common Name (CN)	ANF AC Ecuador Intermediate CA	Sí		OID 2.5.4.3

1.4.6.Organizational Unit (OU)	No aplica	No		
1.5. Validity		Sí		
1.5.1. Not Before	Fecha de inicio de validez	Sí		YYMMDDHHMMSSZ
1.5.2. Not After	Fecha de expiración	Sí		YYMMDDHHMMSSZ
1.6. Subject		Sí		
1.6.1. Country Name (C)	País donde reside de la Persona Jurídica (Pública o Privada) "EC" (ISO 3166)	Sí		OID 2.5.4.6
1.6.2. Locality Name (L)	Localidad de la Persona Jurídica (Pública o Privada) (Ciudad) ej. QUITO	Sí		OID 2.5.4.7
1.6.3. Organization Name (O)	Persona Jurídica (Pública o Privada) de la cual es Representante Legal o Apoderado el Signatario	Sí		OID 2.5.4.10
1.6.4. Organization Identifier	Número de Registro Unico de Contribuyente de la persona jurídica (Pública o Privada) a la que está vinculado el Signatario "VAT(CÓDIGO_PAÍS)-RUC" Ej. VATEC-1716151413001	No		OID 2.5.4.97 codificación acorde la ETSI EN 319 412-1 RFC 5280 establece como no obligatorio
1.6.5. Title	Se especificará el nombre del título o el puesto (cargo) que el Signatario ocupa. Ej. REPRESENTANTE LEGAL O APODERADO	Sí		OID 2.5.4.12
1.6.6. Surname	Apellidos del Signatario (como consta en el documento oficial)	Sí		OID 2.5.4.4
1.6.7. Given Name	Nombres del Signatario (como consta en el documento oficial)	Sí		OID 2.5.4.42
1.6.8. Serial Number	Número de cédula (IDC"Pais"-1716151413) o pasaporte (PAS"País"-A6362611) del Signatario Ej. IDCEC-1716151413 o PASEC-A6362611	Sí		OID 2.5.4.5 Número de documento oficial codificado acorde a ETSI EN 319 412-1
1.6.9. Common Name	Nombres y Apellidos del Signatario	Sí		OID 2.5.4.3
1.7. Subject Public Key Info		Sí		
1.7.1.AlgorithmIdentifier				
1.7.1.1. Algorithm	RSA encryption	Sí		OID 1.2.840.113549.1.1.1
1.7.1.2. Parameters	No aplicable	No		
1.7.2. SubjectPublicKey	Clave pública del Signatario	Sí		Acorde ETSI TS 119 312
2. Extensions				

2.1. Authority Key Identifier	Identificador de la clave del Issuer	No	No	OID 2.5.29.35 (Marcado como NO crítico según EN 319412-2) No es obligatorio siempre y cuando la clave pública de la AC se distribuya en forma de certificado "AUTOFIRMADO"
2.1.1. KeyIdentifier		No		Derivado de la clave pública
2.2. Subject Key Identifier	Identificador de la clave del Subject	Sí	No	OID 2.5.29.14 (Marcado como NO crítico según EN 319412-2)
2.2.1. KeyIdentifier		Sí		Derivado de la clave pública
2.3. Key Usage		Sí	Sí	OID 2.5.29.15
2.3.1. Digital Signature	Seleccionado "1"	Sí		
2.3.2. Content commintment	Seleccionado "1"	Sí		
2.3.3. Key Encipherment	Seleccionado "1"	Sí		
2.3.4. Data Encipherment	No seleccionado. "0"			
2.3.5. Key Agreement	No seleccionado. "0"			
2.3.6. Key Certificate Signature	No seleccionado. "0"			
2.3.7. CRL Signature	No seleccionado. "0"			
2.3.8. Encipher Only	No seleccionado. "0"			
2.3.9. Decipher Only	No seleccionado. "0"			
2.4. Certificate Policies		Si	No	OID 2.5.29.32 (Marcado como NO crítico según EN 319412-2)
2.4.1. Policy Information		Sí		
2.4.1.1. Policy Identifier	1.3.6.1.4.1.37442.2.3.1	Sí		OID 1.3.6.1.5.5.7.2.1 URL de la Política de Certificados de la Entidad Acreditada
2.4.1.2. Policy Qualifiers		Sí		
2.4.1.1.1 CPS URI	https://anf.ec	Sí		OID 1.3.6.1.5.5.7.2.1 URL de la Política de Certificados de la Entidad Acreditada

2.4.1.1.2. User Notice/Explicit text	CERTIFICADO DE REPRESENTANTE LEGAL EN ARCHIVO	Sí		OID 1.3.6.1.5.5.7.2.2 Texto indicativo
2.5. Subject Alternative Names		No	No	OID 2.5.29.17 (Marcado como NO crítico según EN 319412-2)
2.5.1. rfc822Name	Correo electrónico del Signatario "nombreapellido@example.com.ec"	Sí		
2.6. Extended Key Usage		Sí	No	OID 2.5.29.37 (Marcado como NO crítico según EN 319412-2)
2.6.1. clientAuth	Presente (1.3.6.1.5.5.7.3.2)	Sí		Transport Layer Security (TLS) World Wide Web (WWW) client authentication
2.6.2. Email protection	Presente (1.3.6.1.5.5.7.3.4)	No		Sólo se activa si se incluye el correo electrónico del Signatario
2.7. cRLDistributionPoint		No	No	OID 2.5.29.31 (Marcado como NO crítico según EN 319412-2)
2.7.1. distributionPoint	http://crl.anf.es/crl/ANFACEcuadorIntermediateCA.crl	Sí		http (http://) IETF RFC 7230-7235 [3] or ldap (ldap://) IETF RFC 4516 [4] scheme
2.7.2. distributionPoint	No aplica	No		http (http://) IETF RFC 7230-7235 [3] or ldap (ldap://) IETF RFC 4516 [4] scheme
2.8. Authority Information Access		Sí	No	OID 1.3.6.1.5.5.7.1.1 (Marcado como NO crítico según EN 319412-2)
2.8.1. Access Description		Sí		
2.8.1.1. Access Method	id-ad-ocsp	Sí		OID 1.3.6.1.5.5.7.48.1
2.8.1.1.1 Access Location	http://ocsp.anf.es/spain/AV	Sí		URL de acceso al OCSP (http://) IETF RFC 7230-7235 [3] or https (https://) IETF RFC 2818 [5]
2.8.1.1.2. Access Location	No aplica	No		URL de acceso al OCSP (http://) IETF RFC 7230-7235 [3] or https (https://) IETF RFC 2818 [5]
2.8.2. Access Description		No		No es obligatorio siempre y cuando incluya la ubicación de acceso al OCSP
2.8.2.1. Access Method	id-ad-calssuers	No		OID 1.3.6.1.5.5.7.48.2

2.8.2.1.1 Access Location	http://crl.anf.es/certificates-download/ANFACEcuadorIntermediateCA.cer	No		URL acceso a certificado de la CA (http://) IETF RFC 7230-7235 [3] or https (https://) IETF RFC 2818 [5]
2.9. Basic Constraints		Sí	Sí	OID 2.5.29.19
2.9.1. cA	FALSE	Sí		

REPRESENTANTE LEGAL EN DSCF				
Campo	**en Dispositivo Seguro de Creación de Firma DSCF**	**Oblig.**	**Crít.**	**Observaciones OID 1.3.6.1.4.1.37442.2.3.2**
De Representante Legal	**Autenticación y Firma**			
1. Basic estructure				
1.1. Version	V3	Sí		Versión 3. X.509 v3
1.2. Serial Number	Establecido automáticamente por la AC. Número identificativo único del certificado.	Sí		No puede ser un número negativo ni 0.
1.3. Signature Algorithm		Sí		
1.3.1. Algorithm	SHA-256 with RSA Signature	Sí		1.2.840.113549.1.1.11
1.3.2. Parameters	No aplicable	No		
1.4. Issuer		Sí		
1.4.1. Country Name (C)	EC	Sí		OID 2.5.4.6
1.4.2. Organization Name (O)	ANFAC AUTORIDAD DE CERTIFICACION ECUADOR C.A.	Sí		OID 2.5.4.10
1.4.3. Locality Name (L)	QUITO	Sí		OID 2.5.4.7
1.4.4. Organization Identifier	VATEC-1792601215001	No		OID 2.5.4.97 codificación acorde la ETSI EN 319 412-1 RFC 5280 establece como no obligatorio
1.4.5. Common Name (CN)	ANF AC Ecuador Intermediate CA	Sí		OID 2.5.4.3
1.4.6. Organizational Unit (OU)	No aplica	No		
1.5. Validity		Sí		
1.5.1. Not Before	Fecha de inicio de validez	Sí		YYMMDDHHMMSSZ
1.5.2. Not After	Fecha de expiración	Sí		YYMMDDHHMMSSZ
1.6. Subject		Sí		
1.6.1. Country Name	País donde reside de la Persona Jurídica (Pública o Privada) "EC" (ISO 3166)	Sí		OID 2.5.4.6
1.6.2. Locality Name (L)	Localidad de la Persona Jurídica (Pública o Privada) (Ciudad) ej. QUITO	Sí		OID 2.5.4.7

1.6.3. Organization Name	Persona Jurídica (Pública o Privada) de la cual es Representante Legal o Apoderado el Signatario	Sí		OID 2.5.4.10
1.6.4. Organization Identifier	Número de Registro Unico de Contribuyente de la persona jurídica (Pública o Privada) a la que está vinculado el Signatario "VAT(CÓDIGO_PAÍS)-RUC" Ej. VATEC-1716151413001	No		OID 2.5.4.97 codificación acorde la ETSI EN 319 412-1 RFC 5280 establece como no obligatorio
1.6.5. Title	Se especificará el nombre del título o el puesto (cargo) que el Signatario ocupa. Ej. REPRESENTANTE LEGAL O APODERADO	Sí		OID 2.5.4.12
1.6.6. Surname	Apellidos del Signatario (como consta en el documento oficial)	Sí		OID 2.5.4.4
1.6.7. Given Name	Nombres del Signatario (como consta en el documento oficial)	Sí		OID 2.5.4.42
1.6.8. Serial Number	Número de cédula (IDC"Pais"-1716151413) o pasaporte (PAS"País"-A6362611) del Signatario Ej. IDCEC-1716151413 o PASEC-A6362611	Sí		OID 2.5.4.5
1.6.9. Common Name	Nombres y Apellidos del Signatario	Sí		OID 2.5.4.3
1.7. Subject Public Key Info		Sí		
1.7.1. AlgorithmIdentifier				
1.7.1.1. Algorithm	RSA encryption	Sí		OID 1.2.840.113549.1.1.1
1.7.1.2. Parameters	No aplicable	No		
1.7.2. SubjectPublicKey	Clave pública del Signatario	Sí		Acorde ETSI TS 119 312
2. Extensions				
2.1. Authority Key Identifier	Identificador de la clave del Issuer	No	No	OID 2.5.29.35 (Marcado como NO crítico según EN 319412-2) No es obligatorio siempre y cuando la clave pública de la AC se distribuya en forma de certificado "AUTOFIRMADO"
2.1.1. KeyIdentifier		No		Derivado de la clave pública
2.2. Subject Key Identifier	Identificador de la clave del Subject	Sí	No	OID 2.5.29.14 (Marcado como NO crítico según EN 319412-2)
2.2.1. KeyIdentifier		Sí		Derivado de la clave pública
2.3. Key Usage		Sí	Sí	OID 2.5.29.15
2.3.1. Digital Signature	Seleccionado "1"	Sí		
2.3.2. Content commintment	Seleccionado "1"	Sí		
2.3.3. Key Encipherment	Seleccionado "1"	Sí		

2.3.4. Data Encipherment	No seleccionado. "0"			
2.3.5. Key Agreement	No seleccionado. "0"			
2.3.6. Key Certificate Signature	No seleccionado. "0"			
2.3.7. CRL Signature	No seleccionado. "0"			
2.3.8. Encipher Only	No seleccionado. "0"			
2.3.9. Decipher Only	No seleccionado. "0"			
2.4. Certificate Policies		Si	No	OID 2.5.29.32 (Marcado como NO crítico según EN 319412-2)
2.4.1. Policy Information		Sí		
2.4.1.1. Policy Identifier	1.3.6.1.4.1.37442.2.3.2	Sí		Identificador de la política de la AC
2.4.1.2. Policy Qualifiers		Sí		
2.4.1.1.1 CPS URI	https://www.anf.ec	Sí		OID 1.3.6.1.5.5.7.2.1 URL de la Política de Certificados de la Entidad Acreditada
2.4.1.1.2. User Notice/Explicit text	CERTIFICADO DE REPRESENTANTE LEGAL EN DISPOSITIVO SEGURO DE CREACIÓN DE FIRMA - DSCF	Sí		OID 1.3.6.1.5.5.7.2.2 Texto indicativo
2.5. Subject Alternative Names		No	No	OID 2.5.29.17 (Marcado como NO crítico según EN 319412-2)
2.5.1. rfc822Name	Correo electrónico del Signatario "nombreapellido@example.com.ec"	Sí		
2.6. Extended Key Usage		Sí	No	OID 2.5.29.37 (Marcado como NO crítico según EN 319412-2)
2.6.1. clientAuth	Presente (1.3.6.1.5.5.7.3.2)	Sí		Transport Layer Security (TLS) World Wide Web (WWW) client authentication
2.6.2. Email protection	Presente (1.3.6.1.5.5.7.3.4)	No		Sólo se activa si se incluye el correo electrónico del Signatario
2.7. cRLDistributionPoint		No	No	OID 2.5.29.31 (Marcado como NO crítico según EN 319412-2
2.7.1. distributionPoint	http://crl.anf.es/crl/ANFACEcuadorIntermediateCA.crl	Sí		http (http://) IETF RFC 7230-7235 [3] or ldap (ldap://) IETF RFC 4516 [4] scheme

2.7.2. distributionPoint	No aplica	No		http (http://) IETF RFC 7230-7235 [3] or ldap (ldap://) IETF RFC 4516 [4] scheme
2.8. Authority Information Access		Sí	No	OID 1.3.6.1.5.5.7.1.1 (Marcado como NO crítico según EN 319412-2)
2.8.1. Access Description		Sí		
2.8.1.1. Access Method	id-ad-ocsp	Sí		OID 1.3.6.1.5.5.7.48.1
2.8.1.1.1 Access Location	http://ocsp.anf.es/spain/AV	Sí		URL de acceso al OCSP (http://) IETF RFC 7230-7235 [3] or https (https://) IETF RFC 2818 [5]
2.8.1.1.2. Access Location	No aplica	No		URL de acceso al OCSP (http://) IETF RFC 7230-7235 [3] or https (https://) IETF RFC 2818 [5]
2.8.2. Access Description		No		No es obligatorio siempre y cuando incluya la ubicación de acceso al OCSP
2.8.2.1. Access Method	id-ad-calssuers	No		OID 1.3.6.1.5.5.7.48.2
2.8.2.1.1 Access Location	http://crl.anf.es/certificates-download/ANFACEcuadorIntermediateCA.cer	No		URL acceso a certificado de la CA (http://) IETF RFC 7230-7235 [3] or https (https://) IETF RFC 2818 [5]
2.9. Basic Constraints		Sí	Sí	OID 2.5.29.19
2.9.1. cA	FALSE	Sí		

SELLO ELECTRÓNICO EN ARCHIVO				
Campo	**en Archivo**	**Oblig.**	**Crít.**	**Observaciones OID 1.3.6.1.4.1.37442.2.4.1**
Cert SELLO ELECTRÓNICO	**Autenticación y Firma**			
1. Basic estructure				
1.1. Version	V3	Sí		Versión 3. X.509 v3
1.2. Serial Number	Establecido automáticamente por la AC. Número identificativo único del certificado.	Sí		No puede ser un número negativo ni 0.
1.3. Signature Algorithm		Sí		
1.3.1. Algorithm	SHA-256 with RSA Signature	Sí		1.2.840.113549.1.1.11
1.3.2. Parameters	No aplicable	No		

1.4. Issuer		Sí		
1.4.1. Country Name (C)	EC	Sí		OID 2.5.4.6
1.4.2. Locality Name (L)	QUITO	Sí		OID 2.5.4.7
1.4.3. Organization Name (O)	ANFAC AUTORIDAD DE CERTIFICACION ECUADOR C.A.	Sí		OID 2.5.4.10
1.4.4. Organization Identifier	VATEC-1792601215001	No		OID 2.5.4.97 codificación acorde la ETSI EN 319 412-1 RFC 5280 establece como no obligatorio
1.4.5. Common Name (CN)	ANF AC Ecuador Intermediate CA	Sí		OID 2.5.4.3
1.4.6. Organizational Unit (OU)	No aplica	No		OID 2.5.4.11
1.5. Validity		Sí		
1.5.1. Not Before	Fecha de inicio de validez	Sí		YYMMDDHHMMSSZ
1.5.2. Not After	Fecha de expiración	Sí		YYMMDDHHMMSSZ
1.6. Subject		Sí		
1.6.1. Country Name (C)	País donde se encuentra registrada la Persona Jurídica (Pública o Privada) Titular de la Firma "EC" (ISO 3166)	Sí		OID 2.5.4.6
1.6.2. Locality Name (L)	Localidad de la Persona Jurídica (Pública o Privada) Titular de la Firma (Ciudad) ej. QUITO	Sí		OID 2.5.4.7
1.6.3. Organization Name (O)	Nombre de la Persona Jurídica (Pública o Privada) Titular de la Firma ej. "CORPORACIÓN FAVORITA"	Sí		OID 2.5.4.10
1.6.4. Organizational Unit Name (OU)	Se especificará el Departamento o Área a la que pertenece el Signatario	No		OID 2.5.4.11
1.6.5. Organization Identifier	Número de Registro Unico de Contribuyente de la Persona Jurídica (Pública o Privada) Titular de la Firma a la que está vinculado el Sello Electrónico "VAT(CÓDIGO_PAÍS)- RUC" Ej. VATEC-1716151413001	No		OID 2.5.4.97 codificación acorde la ETSI EN 319 412-1 RFC 5280 establece como no obligatorio
1.6.6. Serial Number	Número de Registro Unico de Contribuyente de la Persona Jurídica (Pública o Privada) ej."1716151413001"	Sí		OID 2.5.4.5
1.6.7. Common Name	Descripción del uso que se le dará al sello electrónico. Ej. RECEPCIÓN DE DOCUMENTOS EN VENTANILLA UNICA	Sí		OID 2.5.4.3
1.6.8. Surname	Apellidos del Signatario que estará vinculado el sello (como consta en el documento oficial)	Si		OID 2.5.4.4

1.6.9. Given Name	Nombres del Signatario que estará vinculado el sello (como consta en el documento oficial)	Si		OID 2.5.4.42
1.7. Subject Public Key Info		Sí		
1.7.1. AlgorithmIdentifier				
1.7.1.1. Algorithm	RSA encryption	Sí		OID 1.2.840.113549.1.1.1
1.7.1.2. Parameters	No aplicable	No		
1.7.2. SubjectPublicKey	Clave pública del Signatario	Sí		Acorde ETSI TS 119 312
2. Extensions				
2.1. Authority Key Identifier	Identificador de la clave del Issuer	No	No	OID 2.5.29.35 (Marcado como NO crítico según EN 319412-2) No es obligatorio siempre y cuando la clave pública de la AC se distribuya en forma de certificado "AUTOFIRMADO"
2.1.1. KeyIdentifier		No		Derivado de la clave pública
2.2. Subject Key Identifier	Identificador de la clave del Subject	Sí	No	OID 2.5.29.14 (Marcado como NO crítico según EN 319412-2)
2.2.1. KeyIdentifier		Sí		Derivado de la clave pública
2.3. Key Usage		Sí	Sí	OID 2.5.29.15
2.3.1. Digital Signature	Seleccionado "1"	Sí		
2.3.2. Content commintment	Seleccionado "1"	Sí		
2.3.3. Key Encipherment	Seleccionado "1"	Sí		
2.3.4. Data Encipherment	No seleccionado. "0"			
2.3.5. Key Agreement	No seleccionado. "0"			
2.3.6. Key Certificate Signature	No seleccionado. "0"			
2.3.7. CRL Signature	No seleccionado. "0"			
2.3.8. Encipher Only	No seleccionado. "0"			
2.3.9. Decipher Only	No seleccionado. "0"			
2.4. Certificate Policies		Sí	No	OID 2.5.29.32 (Marcado como NO crítico según EN 319412-2)
2.4.1. Policy Information		Sí		

2.4.1.1. Policy Identifier	1.3.6.1.4.1.37442.2.4.1	Sí		Identificador de la política de AC
2.4.1.2. Policy Qualifiers		Sí		
2.4.1.1.1 CPS URI	https://www.anf.ec	Sí		OID 1.3.6.1.5.5.7.2.1 URL de la Política de Certificados de la Entidad Acreditada
2.4.1.1.2. User Notice/Explicit text	"CERTIFICADO DE SELLO ELECTRONICO EN ARCHIVO"	Sí		OID 1.3.6.1.5.5.7.2.2 Texto indicativo
2.5. Subject Alternative Names		No	No	OID 2.5.29.17 (Marcado como NO crítico según EN 319412-2)
2.5.1. rfc822Name	Correo electrónico de la Persona Jurídica (Pública o Privada) Titular de la Firma (sello electrónico) "info@example.com.ec"	Si		
2.6. Extended Key Usage		Sí	No	OID 2.5.29.37 (Marcado como NO crítico según EN 319412-2)
2.6.1. clientAuth	Presente (1.3.6.1.5.5.7.3.2)	Si		Transport Layer Security (TLS) World Wide Web (WWW) client authentication
2.6.2. Email protection	Presente (1.3.6.1.5.5.7.3.4)	No		Sólo se activa si se incluye el correo electrónico de la Persona Jurídica (Pública o Privada) Titular de la Firma (sello electrónico)
2.7. cRLDistributionPoint		No	No	OID 2.5.29.31 (Marcado como NO crítico según EN 319412-2
2.7.1. distributionPoint	http://crl.anf.es/crl/ANFACEcuadorIntermediateCA.crl	Sí		http (http://) IETF RFC 7230-7235 [3] or ldap (ldap://) IETF RFC 4516 [4] scheme
2.7.2. distributionPoint	No aplica	No		http (http://) IETF RFC 7230-7235 [3] or ldap (ldap://) IETF RFC 4516 [4] scheme
2.8. Authority Information Access		Sí	No	OID 1.3.6.1.5.5.7.1.1 (Marcado como NO crítico según EN 319412-2)
2.8.1. Access Description		Sí		
2.8.1.1. Access Method	id-ad-ocsp	Sí		OID 1.3.6.1.5.5.7.48.1

2.8.1.1.1 Access Location	http://ocsp.anf.es/spain/AV	Sí		URL de acceso al OCSP (http://) IETF RFC 7230-7235 [3] or https (https://) IETF RFC 2818 [5]
2.8.1.1.2. Access Location	No aplica	No		URL de acceso al OCSP (http://) IETF RFC 7230-7235 [3] or https (https://) IETF RFC 2818 [5]
2.8.2. Access Description		No		No es obligatorio siempre y cuando incluya la ubicación de acceso al OCSP
2.8.2.1. Access Method	id-ad-calssuers	No		OID 1.3.6.1.5.5.7.48.2
2.8.2.1.1 Access Location	http://crl.anf.es/certificates-download/ANFACEcuadorIntermediateCA.cer	No		URL acceso a certificado de la CA (http://) IETF RFC 7230-7235 [3] or https (https://) IETF RFC 2818 [5]
2.9. Basic Constraints		Sí	Sí	OID 2.5.29.19
2.9.1. cA	FALSE	Sí		

SELLO ELECTRÓNICO EN DSCF				
Campo	**en Dispositivo Seguro de Creación de Firma DSCF**	**Oblig.**	**Crít.**	**Observaciones OID 1.3.6.1.4.1.37442.2.4.2**
Cert SELLO ELECTRÓNICO	**Autenticación y Firma**			
1. Basic estructure				
1.1. Version	V3	Sí		Versión 3. X.509 v3
1.2. Serial Number	Establecido automáticamente por la AC. Número identificativo único del certificado.	Sí		No puede ser un número negativo ni 0.
1.3. Signature Algorithm		Sí		
1.3.1. Algorithm	SHA-256 with RSA Signature	Sí		1.2.840.113549.1.1.11
1.3.2. Parameters	No aplicable	No		
1.4. Issuer		Sí		
1.4.1. Country Name (C)	EC	Sí		OID 2.5.4.6
1.4.2. Locality Name (L)	QUITO	Si		OID 2.5.4.7
1.4.3. Organization Name (O)	ANFAC AUTORIDAD DE CERTIFICACION ECUADOR C.A.	Sí		OID 2.5.4.10
1.4.4. Organization Identifier	VATEC-1792601215001	No		OID 2.5.4.97 codificación acorde la ETSI EN 319 412-1 RFC 5280 establece como no obligatorio
1.4.5. Common Name (CN)	ANF AC Ecuador Intermediate CA	Sí		OID 2.5.4.3
1.4.6. Organizational Unit (OU)	No aplica	No		OID 2.5.4.11
1.5. Validity		Sí		
1.5.1. Not Before	Fecha de inicio de validez	Sí		YYMMDDHHMMSSZ
1.5.2. Not After	Fecha de expiración	Sí		YYMMDDHHMMSSZ
1.6. Subject		Sí		
1.6.1. Country Name (C)	País donde se encuentra registrada la Persona Jurídica (Pública o Privada) Titular de la Firma "EC" (ISO 3166)	Sí		OID 2.5.4.6

1.6.2. Locality Name (L)	Localidad de la Persona Jurídica (Pública o Privada) Titular de la Firma (Ciudad) ej. QUITO	Sí		OID 2.5.4.7
1.6.3. Organization Name (O)	Nombre de la Persona Jurídica (Pública o Privada) Titular de la Firma ej. "CORPORACIÓN FAVORITA"	Sí		OID 2.5.4.10
1.6.4. Organizational Unit Name (OU)	Se especificará el Departamento o Área a la que pertenece el Signatario	No		OID 2.5.4.11
1.6.5. Organization Identifier	Número de Registro Unico de Contribuyente de la Persona Jurídica (Pública o Privada) Titular de la Firma a la que está vinculado el Sello Electrónico "VAT(CÓDIGO_PAÍS)- RUC" Ej. VATEC-1716151413001	No		OID 2.5.4.97 codificación acorde la ETSI EN 319 412-1 RFC 5280 establece como no obligatorio
1.6.6. Serial Number	Número de Registro Unico de Contribuyente de la Persona Jurídica (Pública o Privada) ej."1716151413001"	Sí		OID 2.5.4.5
1.6.4. Common Name	Descripción del uso que se le dará al sello electrónico. Ej. RECEPCIÓN DE DOCUMENTOS EN VENTANILLA UNICA	Sí		OID 2.5.4.3
1.6.8. Surname	Apellidos del Signatario que estará vinculado el sello (como consta en el documento oficial)	Si		OID 2.5.4.4
1.6.8. Given Name	Nombres del Signatario que estará vinculado el sello (como consta en el documento oficial)	Si		OID 2.5.4.42
1.7. Subject Public Key Info		Sí		
1.7.1. AlgorithmIdentifier				
1.7.1.1. Algorithm	RSA encryption	Sí		OID 1.2.840.113549.1.1.1
1.7.1.2. Parameters	No aplicable	No		
1.7.2. SubjectPublicKey	Clave pública del Signatario	Sí		Acorde ETSI TS 119 312
2. Extensions				
2.1. Authority Key Identifier	Identificador de la clave del Issuer	No	No	OID 2.5.29.35 (Marcado como NO crítico según EN 319412-2) No es obligatorio siempre y cuando la clave pública de la AC se distribuya en forma de certificado "AUTOFIRMADO"
2.1.1. KeyIdentifier		No		Derivado de la clave pública
2.2. Subject Key Identifier	Identificador de la clave del Subject	Sí	No	OID 2.5.29.14 (Marcado como NO crítico según EN 319412-2)
2.2.1. KeyIdentifier		Sí		Derivado de la clave pública

2.3. Key Usage		Sí	Sí	OID 2.5.29.15
2.3.1. Digital Signature	Seleccionado "1"	Sí		
2.3.2. Content commintment	Seleccionado "1"	Sí		
2.3.3. Key Encipherment	Seleccionado "1"	Sí		
2.3.4. Data Encipherment	No seleccionado. "0"			
2.3.5. Key Agreement	No seleccionado. "0"			
2.3.6. Key Certificate Signature	No seleccionado. "0"			
2.3.7. CRL Signature	No seleccionado. "0"			
2.3.8. Encipher Only	No seleccionado. "0"			
2.3.9. Decipher Only	No seleccionado. "0"			
2.4. Certificate Policies		Si	No	OID 2.5.29.32 (Marcado como NO crítico según EN 319412-2)
2.4.1. Policy Information		Sí		
2.4.1.1. Policy Identifier	1.3.6.1.4.1.37442.2.4.2	Sí		Identificador de la política de AC
2.4.1.2. Policy Qualifiers		Sí		
2.4.1.1.1 CPS URI	https://www.anf.ec	Sí		OID 1.3.6.1.5.5.7.2.1 URL de la Política de Certificados de la Entidad Acreditada
2.4.1.1.2. User Notice/Explicit text	CERTIFICADO DE SELLO ELECTRONICO EN DISPOSITIVO SEGURO DE CREACIÓN DE FIRMA - DSCF	Sí		OID 1.3.6.1.5.5.7.2.2 Texto indicativo
2.5. Subject Alternative Names		No	No	OID 2.5.29.17 (Marcado como NO crítico según EN 319412-2)
2.5.1. rfc822Name	Correo electrónico de la Persona Jurídica (Pública o Privada) Titular de la Firma (sello electrónico) "info@example.com.ec"	No		
2.6. Extended Key Usage		Sí	No	OID 2.5.29.37 (Marcado como NO crítico según EN 319412-2)
2.6.1. clientAuth	Presente (1.3.6.1.5.5.7.3.2)	Sí		Transport Layer Security (TLS) World Wide Web (WWW) client authentication

2.6.2. Email protection	Presente (1.3.6.1.5.5.7.3.4)	No		Sólo se activa si se incluye el correo electrónico de la Persona Jurídica (Pública o Privada) Titular de la Firma (sello electrónico)
2.7.cRLDistributionPoint		No	No	OID 2.5.29.31 (Marcado como NO crítico según EN 319412-2
2.7.1. distributionPoint	http://crl.anf.es/crl/ANFACEcuadorIntermediateCA.crl	Sí		http (http://) IETF RFC 7230-7235 [3] or ldap (ldap://) IETF RFC 4516 [4] scheme
2.7.2. distributionPoint	No aplica	No		http (http://) IETF RFC 7230-7235 [3] or ldap (ldap://) IETF RFC 4516 [4] scheme
2.8. Authority Information Access		Sí	No	OID 1.3.6.1.5.5.7.1.1 (Marcado como NO crítico según EN 319412-2)
2.8.1. Access Description		Sí		
2.8.1.1. Access Method	id-ad-ocsp	Sí		OID 1.3.6.1.5.5.7.48.1
2.8.1.1.1 Access Location	http://ocsp.anf.es/spain/AV	Sí		URL de acceso al OCSP (http://) IETF RFC 7230-7235 [3] or https (https://) IETF RFC 2818 [5]
2.8.1.1.2. Access Location	No aplica	No		URL de acceso al OCSP (http://) IETF RFC 7230-7235 [3] or https (https://) IETF RFC 2818 [5]
2.8.2. Access Description		No		No es obligatorio siempre y cuando incluya la ubicación de acceso al OCSP
2.8.2.1. Access Method	id-ad-calssuers	No		OID 1.3.6.1.5.5.7.48.2

2.8.2.1.1 Access Location	http://crl.anf.es/certificates-download/ANFACEcuadorIntermediateCA.cer	No		URL acceso a certificado de la CA (http://) IETF RFC 7230-7235 [3] or https (https://) IETF RFC 2818 [5]
2.9. Basic Constraints		Sí	Sí	OID 2.5.29.19
2.9.1. cA	FALSE	Sí		

7.1.3. Identificadores de Objeto de los algoritmos utilizados

El identificador de algoritmo (AlgorithmIdentifier) que emplea ANF AC para firmar los certificados es SHA-256/RSA.

OID	Nombre	Descripción
1.2.840.113549.1.1.11	SHA256withRSAEncryption	OID del algoritmo de firma
1.2.840.113549.1.1.1	RSAEncryption	OID de Clave pública

ANF AC no usa ECDSA.

7.1.4. Formatos de nombres

Todos los certificados contienen un nombre distinguido (Distinguished Name) X.500, en el campo Subject Name. Un "Distinguished Name" que ha sido utilizado en un certificado nunca será reasignado a otra entidad. El subject y el issuer identifican a la persona (física o jurídica) o dispositivo, y deberán tener significado en el sentido de que la CA dispone de la evidencia de la asociación entre estos nombres o pseudónimos y las entidades a las que están asignados. Los nombres no pueden inducir a confusión.

El contenido del campo DN del emisor del certificado coincide con el DN del sujeto de la CA emisora para admitir el encadenamiento de nombres como se especifica en RFC 5280, sección 4.1.2.4.

Los atributos que componen el nombre diferenciado del campo subject son los recogidos en el apartado correspondiente al perfil del certificado.

En algunos tipos de certificados el campo subjectAltName, incluye información del sujeto.

En todos los certificados de identidad de la entidad final, el campo Common Name contiene el nombre completo del suscriptor del certificado.

El perfil se basa en las recomendaciones IETF RFC 5280, y el estándar ITU-T X.509. ETSI ha elaborado normas europeas en cumplimiento del Mandato M/460 de la Comisión Europea para racionalizar los estándares en torno a la firma electrónica. La familia ETSI EN 319 412 especifica el contenido de los certificados expedidos a personas físicas, jurídicas o certificados de sitios web.

La Política de Certificación a la que se somete cada certificado determina especificidades concretas al respecto.

7.1.5. Restricciones de nombres

No aplicable. No se emplean restricciones de nombres.

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

Los OID de cada certificado incluido en las políticas de certificación de cada tipo de certificado se encuentran detallados en el primer capítulo del presente documento.

7.1.7. Uso de la extensión "Policy Constraints"

No se estipulan restricciones de política.

7.1.8. Sintaxis y semántica de los calificadores de política

La extensión Certificate Policies contiene los siguientes calificadores de política "PolicyQualifier":

- Policy Identifier: Identifica el tipo de perfil de certificado dentro de una determinada política de certificación a la que está asociado.
- Policy Qualifier ID: Identifica la Política de Certificación que le sea de aplicación.
- CPS Pointer: contiene un puntero a la Declaración de Prácticas de Certificación y Políticas publicadas por ANF AC.
- User Notice: Se expresa una declaración realizada por la CA emisora, en la que se hace referencia a determinadas normas legales.

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

La extensión Certificate Policy permite identificar la política a la que se somete el certificado y dónde se pueden encontrar dicha Política de Certificación.

7.1.10. Guía de cumplimentación de campos en los certificados

Según recomendación del documento RFC 5280 (actualizada por RFC 6818), los campos serán codificados en UTF8. En base a ello se codifican grupos de caracteres internacionales, incluyendo caracteres del alfabeto latino con signos diacríticos ("Ñ", "ñ", "Ç", "ç", "Ü", "ü", etc.) como, por ejemplo, el carácter eñe (ñ), que se representa en Unicode como 0x00F1.

Además, y con el fin de establecer un marco común en todos los certificados emitidos en el ámbito de la PKI de ANF AC, se tratará de mantener las siguientes recomendaciones en la emisión de certificados:

- Todos los literales se introducen en mayúsculas, con las excepciones del nombre de dominio/subdominio y el correo electrónico, que estarán en minúsculas.
- Se codifican los nombres tal y como aparecen en la documentación acreditativa.
- Respecto a los apellidos de personas naturales, se debe incluir obligatoriamente el PRIMER Y SEGUNDO APELLIDO, separados únicamente por un espacio en blanco, de acuerdo con lo indicado en la cédula de identidad o en el pasaporte. En caso de no existir el segundo apellido, se dejará en blanco (sin ningún carácter).
- Incluir obligatoriamente el número de cédula de identidad, documento nacional o pasaporte, junto con el dígito de control, en su caso, de acuerdo con lo indicado en el documento oficial.

- Incluir delante del número de la cédula “IDC + Pais"(Ej. IDCEC-1716151413) o pasaporte “PAS + País" (Ej. PASEC-A6362611)
- 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.
- El campo “User Notice” no tendrá más de 200 caracteres.
- Cada Política de Certificación podrá definir reglas y limitaciones específicas.

7.1.11. Campos propietarios

Se han asignado identificadores ObjectId 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.

A continuación, se muestran las extensiones propietarias que ANF AC puede introducir en los certificados expedidos. Junto con el OID asignado se especifica qué valor contiene:

OID	Valor contenido
1.3.6.1.4.1. 37442.10.1	Nombre del representante legal (suscriptor)
1.3.6.1.4.1. 37442.10.2	Primer apellido del representante legal (suscriptor)
1.3.6.1.4.1. 37442.10.3	Segundo apellido del representante legal (suscriptor)
1.3.6.1.4.1. 37442.10.4	RUC del representante legal (suscriptor)
1.3.6.1.4.1. 37442.10.5	Documento acreditativo del representante legal (suscriptor)
1.3.6.1.4.1. 37442.10.6	Poderes mancomunados (sólo en caso de serlo)
1.3.6.1.4.1. 37442.10.7	Dirección correo electrónico representante legal (suscriptor)
1.3.6.1.4.1. 37442.10.8	Tipo de cédula de identidad presentada por el suscriptor
1.3.6.1.4.1. 37442.10.9	Nacionalidad (suscriptor)
1.3.6.1.4.1. 37442.10.10	Hash del acta de mandato o poder de representación, digitalizada del original.
1.3.6.1.4.1. 37442.10.10.1	Enlace para la descarga del acta de mandato o poder de representación, digitalizada del original.
1.3.6.1.4.1. 37442.11	Nombre completo de una persona física o jurídica, que otorga una representación al suscriptor
1.3.6.1.4.1. 37442.12	Nombre de pila de la persona física que otorga una representación al suscriptor
1.3.6.1.4.1. 37442.13	Apellidos de la persona natural que otorga una representación al suscriptor
1.3.6.1.4.1. 37442.14	RUC / Cédula de la entidad jurídica o persona natural que otorga una representación al suscriptor

1.3.6.1.4.1. 37442.19	Localizador de la solicitud (secuencial de trámite – identificador Operador AR o RDE que la tramitó)
1.3.6.1.4.1. 37442.19.1	Operador AR que tramitó la solicitud. NOTA: en el caso de certificados de Operador AR, RDE o PKI, este OID corresponde al identificador del operador titular del certificado, reseñado en la parte primera del código)
1.3.6.1.4.1. 37442.20.1	Razón social (suscriptor)
1.3.6.1.4.1. 37442.20.2	RUC (de la razón social)
1.3.6.1.4.1. 37442.20.3	Nombre (suscriptor)
1.3.6.1.4.1. 37442.20.4	Primer apellido (suscriptor)
1.3.6.1.4.1. 37442.20.5	Segundo apellido (suscriptor)
1.3.6.1.4.1. 37442.20.6	RUC (suscriptor)
1.3.6.1.4.1. 37442.20.7	Dirección (suscriptor)
1.3.6.1.4.1. 37442.20.8	Tipo de cédula de identidad presentada por el suscriptor
1.3.6.1.4.1. 37442.20.13	Nacionalidad (suscriptor)
1.3.6.1.4.1. 37442.20.10	Código numérico que define el tratamiento con el que hay que dirigirse al suscriptor
1.3.6.1.4.1. 37442.29.1	Nombre del Responsable del Certificado
1.3.6.1.4.1. 37442.29.2	Primer Apellido del Responsable del Certificado
1.3.6.1.4.1. 37442.29.3	Segundo Apellido del Responsable del Certificado
1.3.6.1.4.1. 37442.29.4	RUC del Responsable del Certificado
1.3.6.1.4.1. 37442.29.5	E-mail del Responsable del Certificado
1.3.6.1.4.1. 37442.29.6	Cargo, título, rol del Responsable del Certificado
1.3.6.1.4.1. 37442.29.7	Departamento al que está adscrito el Responsable del Certificado
1.3.6.1.4.1. 37442.29.8	Tipo de cédula de identidad presentada por el responsable del certificado
1.3.6.1.4.1. 37442.29.9	Nacionalidad del responsable del certificado
1.3.6.1.4.1. 37442.29.10	Dirección donde reside el responsable del certificado
1.3.6.1.4.1. 37442.29.11	Población donde reside el responsable del certificado
1.3.6.1.4.1. 37442.29.12	Provincia donde reside el responsable del certificado
1.3.6.1.4.1. 37442.29.13	CP donde reside el responsable del certificado
1.3.6.1.4.1. 37442.29.14	País donde reside el responsable del certificado
1.3.6.1.4.1. 37442.29.15	Teléfono fijo del responsable del certificado
1.3.6.1.4.1. 37442.29.16	Teléfono del responsable del certificado

1.3.6.1.4.1. 37442.29.17	Fax del responsable del certificado
1.3.6.1.4.1. 37442.29.18	Mail del responsable del certificado
1.3.6.1.4.1. 37442.30.1	País al que corresponde la emisión del certificado.
1.3.6.1.4.1. 37442.40.1	Calificación con la que ha sido emitido el certificado
1.3.6.1.4.1. 37442.41.1	Límite de responsabilidad asumido por la CA
1.3.6.1.4.1. 37442.41.2	Limitación de uso del certificado por concepto
1.3.6.1.4.1. 37442.41.3	Limitación de uso del certificado por importe
1.3.6.1.4.1. 37442.41.4	Limitación de uso del certificado tipo moneda
1.3.6.1.4.1. 37442.42.1	Identificador del Tercero Vinculado al que pertenece el operador AR.
1.3.6.1.4.1. 37442.42.3	Determina que se trata de un RDE “Responsable Dictámenes de Emisión”
1.3.6.1.4.1. 37442.42.8	Nivel seguridad del Operador PKI
1.3.6.1.4.1. 37442.42.9	Determina que se trata de un Operador PKI “Operador Autorizado de la PKI”
1.3.6.1.4.1. 37442.42.11	Nombre del Titular del Tercero Vinculado al cual está adscrito el Operador AR
1.3.6.1.4.1. 37442.42.13	Departamento en el que trabaja el Operador AR en el Tercero Vinculado.
1.3.6.1.4.1. 37442.43	Automatización de limitaciones para procesos automáticos
1.3.6.1.4.1. 37442.45.1	RUC Apoderado 2 (mancomunado)
1.3.6.1.4.1. 37442.45.2	Nombre apoderado 2 (mancomunado)
1.3.6.1.4.1. 37442.45.3	Primer apellido apoderado 2 (mancomunado)
1.3.6.1.4.1. 37442.45.4	Segundo apellido apoderado 2 (mancomunado)
1.3.6.1.4.1. 37442.45.5	Documento acreditativo del apoderamiento
1.3.6.1.4.1. 37442.46	Determina que se trata de un certificado de corta vigencia. Valor de referencia 1.
1.3.6.1.4.1. 37442.47	Determina los días de vigencia de certificados electrónicos para personalizar emisión
1.3.6.1.4.1. 37442.47.1	UUID del Dispositivo de Firma Electrónica que almacena el certificado
1.3.6.1.4.1. 37442.47.3	Si está activo indica que los datos de generación de firma están contenidos en un dispositivo criptográfico
1.3.6.1.4.1. 37442.56.2.1	Lista negra de personas y entidades
1.3.6.1.4.1. 37442.60.1	Sistema de micropagos activado
1.3.6.1.4.1. 37442.60.4	Sistema Pagaré Electrónico activado
1.3.6.1.4.1. 37442.85.1	Hash Entrante del encadenamiento de un Sello Digital de Tiempo

1.3.6.1.4.1. 37442.85.2	Hash Saliente del encadenamiento de un Sello Digital de Tiempo
1.3.6.1.4.1. 37442.90	Aspectos profesionales o empresariales descriptivos de la actividad
1.3.6.1.4.1. 37442.90.1	Otros aspectos relacionados con la calidad del servicio
1.3.6.1.4.1. 37442.90.2	Otros aspectos relacionados con la calidad del servicio
1.3.6.1.4.1. 37442.90.3	Otros aspectos relacionados con la calidad del servicio
1.3.6.1.4.1. 37442.91	Fecha creación empresa
1.3.6.1.4.1. 37442.91.1	Forma Jurídica del suscriptor
1.3.6.1.4.1. 37442.91.2	Año de origen de la actividad
1.3.6.1.4.1. 37442.92	Marcas o denominaciones comerciales propias
1.3.6.1.4.1. 37442.92.1	Marcas que distribuye sufijo 1
1.3.6.1.4.1. 37442.92.2	Marcas que distribuye sufijo 2
1.3.6.1.4.1. 37442.92.3	Marcas que distribuye sufijo 3
1.3.6.1.4.1. 37442.93	Ámbito geográfico en que desarrolla su actividad
1.3.6.1.4.1. 37442.94	Direcciones de sedes, teléfonos, fax, sitios web de localización
1.3.6.1.4.1. 37442.94.1	Delegaciones sufijo 1
1.3.6.1.4.1. 37442.94.2	Delegaciones sufijo 2
1.3.6.1.4.1. 37442.94.3	Delegaciones sufijo 3
1.3.6.1.4.1. 37442.95	Compañías con las que se relaciona
1.3.6.1.4.1. 37442.95.1	Compañías con las que se relaciona sufijo 1
1.3.6.1.4.1. 37442.95.2	Compañías con las que se relaciona sufijo 2
1.3.6.1.4.1. 37442.95.3	Compañías con las que se relaciona sufijo 3
1.3.6.1.4.1. 37442.96	Entidades bancarias con las que mantiene relaciones
1.3.6.1.4.1. 37442.96.1	Cuentas corrientes, SWIFT
1.3.6.1.4.1. 37442.97	Información económica referida a su actividad
1.3.6.1.4.1. 37442.97.1	Información económica referida a su actividad sufijo 1
1.3.6.1.4.1. 37442.97.2	Información económica referida a su actividad sufijo 2
1.3.6.1.4.1. 37442.97.3	Información económica referida a su actividad sufijo 3
1.3.6.1.4.1. 37442.98	Número empleados
1.3.6.1.4.1. 37442.99	Número de distribuidores
1.3.6.1.4.1. 37442.600	Contiene la versión de la aplicación AR Manager utilizada para tramitar la solicitud de certificado.

QcLimitValue (OID 0.4.0. 37442.1.2) 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 $.

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 de forma absoluta directamente. P.ej. 1000 $. 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

7.2. Perfil de CRL

Las CRLs emitidas por ANF AC son conformes a las siguientes normas:

- Internet X.509 Public Key Infrastructure Certificate and CRL Profile (RFC 5280) abril 2002
- Internet X.509 Public Key Infrastructure Authority Information Access Certificate Revocation List (CRL) Extension (RFC 4325) diciembre 2005
- Update to DirectoryString Processing in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile (RFC 4630) agosto 2006.

7.2.1. Version number(s)

Versión 2.

7.2.2. CRL y extensiones

Los campos y extensiones utilizadas son las siguientes:

Campo	Valores	Obligatorio	Crítico
Versión	V2 (versión del estándar X.509)	SI	NO
Authority key Identifier	Identificador de la clave del emisor	SI	NO
Número de serie CRL	Código único con respecto a esa determinada jerarquía del emisor	SI	NO
Algoritmo de firma	Sha1WithRSAEncryption	SI	NO
Algoritmo de hash	Sha1	SI	NO
Emisor (Issuer)	CN = de la CA emisora SERIALNUMBER = RUC de la CA emisora OU = Unidad organizacional de la CA emisora O = Nombre de la CA emisora C =País de la CA emisora	SI	NO
Fecha efectiva de emisión	Fecha de emisión de la CRL	SI	NO
Fecha de próxima actualización	Fecha de la próxima emisión de la CRL	SI	NO
Punto de distribución	URL del punto de distribución y tipo de certificados que contiene	SI	NO

Entradas de la CRL	Nº de serie del certificado	SI	NO
	Fecha de revocación	SI	NO
	Código de razón	NO	NO

7.3. Perfil de OCSP

Los certificados emitidos por ANF AC para Respondedores OCSP, son conformes con la norma RFC 6960 “Internet X.509 Public Key Infrastructure Online Certificate Status Protocol-OCSP “.

7.3.1. Version number(s)

Versión 3.

7.3.2. Extensiones OCSP

Campo	Obligatorio	Crítico
Versión	SI	NO
Issuer Alternative name	NO	NO
Authority/Subject Key Identifier	NO	NO
CRL Distribution Point	NO	NO
Key Usage	SI	SI
Enhanced Key Usage	SI	SI

7.3.3. Validación de la Ruta de Certificación

La consulta OCSP verifica toda la Ruta de Certificación y determina el estado de vigencia de cada uno de los certificados de la cadena, hasta alcanzar el máximo nivel superior del Certificado Raíz.

La secuencia de los elementos verificados en la construcción de la Ruta de Certificación contempla como mínimo:

1. Nombre del emisor del certificado verificado. Debe ser igual al nombre del Sujeto en el certificado del emisor.
2. El formato de Certificado debe de ser X.509v3 en la codificación DER.
3. La firma del certificado debe ser verificada con la clave pública del certificado del emisor.
4. El campo “AuthorityKeyIdentifier” del certificado verificado Key Identifier, debe ser igual al “SubjectKeyIdentifier” en el certificado del emisor. Cada certificado debe contener el campo “SubjectKeyIdentifier”.
5. Si el certificado contiene “authorityCertIssuer” verificado en “AuthorityKeyIdentifier”, entonces el nombre debe ser igual al nombre del emisor en el certificado del emisor.

6. Si el certificado contiene “authorityCertSerialNumber” verificado en “AuthorityKeyIdentifier”, “authorityCertSerialNumber” entonces debe ser igual al “serialNumber” en el certificado del emisor.

7. Determina si los certificados de CA “entidad emisora” de la ruta de certificación, incorporan el campo “basicConstraints”, con valor VERDADERO.

8. Si “basicConstraints” es VERDADERO, el certificado puede contener el campo “pathLengthConstraint” que determina el número máximo de certificados de CA que pueden ser encadenados a continuación del certificado verificado. Si el valor es 0, indica que la CA sólo puede emitir certificados de entidad final.

   Si el certificado de CA no contiene el campo “pathLengthConstraint”, quiere decir que no existe restricción en la Ruta de Certificación, salvo que venga restringido por el valor reseñado en un certificado de nivel superior. El parámetro en una CA intermedia tiene que ser un valor inferior al que aparece en una CA de nivel superior.

   Así pues, la longitud de la Ruta de Certificación afecta al número de certificados de CA que se utilizará durante la validación de certificados. La cadena comienza con el certificado de entidad final que se valida y se mueve hacia arriba.

9. El tiempo de control debe estar en el intervalo “no antes, no después” (notBefore, notAfter). El certificado no debe haber caducado en el tiempo de control.

10. El tiempo de control debe estar en el intervalo (no antes, no después) (notBefore, notAfter) –Ninguno de los certificados de niveles inferiores debe de haber sido emitido en un tiempo anterior al momento de emisión del certificado de nivel superior.

11. Se verificará que el uso de la clave “keyUsage” está en coherencia con el tipo de certificado verificado.

12. Si el certificado ha sido emitido con la calificación de cualificado, comprobará si la extensión “QcStatements” está en conformidad con el perfil definido en su correspondiente política, la cual se identifica por el OID incluido en la extensión “PolicyIdentifier”.

La firma de la petición es opcional y depende de lo que decida la Autoridad de Validación OCSP. ANF AC en consultas OCSP sobre servicio WEB no requiere peticiones firmadas, pero puede, según el OCSP, responder consultado, requerir que el suscriptor sea usuario autorizado y esté suscrito al servicio. ANF AC firma las respuestas OCSP con certificado OCSP emitido por la misma organización emisora de los certificados de entidad final.

De acuerdo con lo indicado en la RFC 6960, NONCE criptográficamente une una petición y una respuesta para prevenir los ataques de repetición. El nonce se incluye como uno de los requestExtensions en las solicitudes, mientras que en las respuestas que se incluiría como uno de los responseExtensions. Tanto en la solicitud y en la respuesta, el nonce será identificado por el identificador de objeto id-pkix-ocsp-nonce, mientras que la extnValue es el valor de la nonce.

8. AUDITORÍA DE CUMPLIMIENTO Y OTRAS EVALUACIONES

ANF AC realiza periódicamente procesos de auditoría internos, y contrata a auditores independientes de máximo prestigio para someter a revisión su infraestructura de clave pública.

La verificación de la conformidad con los requisitos de seguridad, se encuentra definida en el documento publicado por ANF AC "Normas y criterios de auditoría de los Servicios de Certificación" (OID 1.3.6.1.4.1.37442.11.1.1)

Se realizan verificaciones "in situ" para determinar si el personal de explotación sigue los procedimientos establecidos.

8.1. Frecuencia o circunstancias de las auditorías

ANF AC somete su PKI anualmente a un proceso de auditoría, además de las auditorías bajo demanda que pueda llevar a cabo bajo su propio criterio, a causa de una sospecha de incumplimiento de alguna medida de seguridad o por un compromiso de claves.

- Auditoría externa de Seguridad Informática. Periodicidad anual. Para envío a ARCOTEL.
- Auditoría protección de datos, anual.
- Auditoría PCI DSS, de forma anual.
- Auditorías Terceros Vinculados, de forma discrecional.
- Auditorías de Sistemas, de forma discrecional.
- Auditoría interna ISO 26000, de forma anual.

8.2. Identidad/Acreditaciones del auditor

La Junta Rectora de la PKI determina para cada control, y según el área sometida a revisión, el personal encargado en llevar a cabo esta operación, asegurándose de que cuenta con la experiencia necesaria y de que se trata de un experto en sistemas de certificación digital.

Las auditorias basadas en normas y estándares ISO, así como auditoría externa de Seguridad Informática, deben ser realizadas por auditores que cuentan con la acreditación necesaria.

8.3. Relación del auditor con la entidad auditada

La Junta Rectora de la PKI puede encomendar la labor de control a auditores internos o externos, pero, en todo caso, funcionalmente independientes del área objeto de fiscalización.

Para la auditoría externa de Seguridad Informática a disposición de ARCOTEL, no podrá auditar la misma entidad por más de cuatro (4) años consecutivos.

8.4. Aspectos cubiertos por la auditoría

El alcance de la auditoría de Seguridad Informática anual de ANF AC incluye:

- Políticas y prácticas,
- Conformidad de la DPC con las políticas publicadas,
- Gestión del ciclo de vida de claves de la CA,
- Gestión del ciclo de vida del certificado,
- Sellado de tiempo,
- Gestión y operación,
- Controles de seguridad y acceso,
- Sistema de seguridad de la información,
- Gestión de incidentes,
- Evaluaciones y análisis de riesgos,
- Recopilación de evidencias,
- Gestión de la continuidad del negocio.
- Planes de Cese,

ANF AC realiza una correcta gestión de seguridad mediante la implementación de un Sistema de Gestión de la Seguridad de la Información de acuerdo a los principios establecidos por la ISO/IEC 27001 que incluye, entre otras, las siguientes medidas:

1. Realizar de forma periódica comprobaciones de seguridad, con el fin de verificar la conformidad con los estándares establecidos.
2. Llevar a cabo una completa gestión de los sucesos de seguridad, con el fin de garantizar su detección, resolución y optimización.
3. Mantener los contactos y relaciones apropiadas con grupos de especial interés en materia de seguridad, como especialistas, foros de seguridad y asociaciones profesionales relacionadas con la seguridad de la información.
4. Planificar adecuadamente el mantenimiento y evolución de los sistemas, con el fin de garantizar en todo momento un rendimiento adecuado y un servicio que cumpla con todas las garantías las expectativas de los usuarios y clientes.

8.5. Acciones tomadas como resultado de las deficiencias

Una vez recibido el informe de la auditoría de cumplimiento llevada a cabo, ANF AC analiza, junto a la entidad que ha ejecutado la auditoría, las posibles deficiencias encontradas, diseñando un plan correctivo que solvente dichas deficiencias y estableciendo su ejecución.

Una vez que las deficiencias sean subsanadas, se realiza una nueva auditoría para confirmar su implantación y la efectividad de las soluciones tomadas.

8.6. Comunicación de resultados

ANF AC comunica los resultados de auditoría a la ARCOTEL y a cualquier entidad externa autorizada por ley, reglamento o acuerdo para recibir una copia de los resultados de la auditoría. ANF AC publica sus Certificaciones de Auditoría anual a más tardar tres (3) meses después del final del período de auditoría. En el caso de demora mayor a tres meses, ANF AC proporcionará una carta explicativa firmada por el auditor cualificado.

Los informes de auditoría serán entregados a la Junta Rectora de la PKI para su análisis. La Junta adoptará las medidas adecuadas según el tipo de incidencia detectado.

8.7. Auditorías internas

ANF AC realizará auditorías internas periódicas de sus operaciones, personal y cumplimiento con esta DPC utilizando una muestra aleatoria de los Certificados emitidos desde la última auditoría interna, como mínimo una vez al año. En la planificación anual de auditorías se audita específicamente la operativa de emisión de los certificados con una muestra mínima de 100 certificados emitidos de cada tipo.

9. ASUNTOS LEGALES Y OTROS

9.1. Tarifas

ANF AC cobra a los suscriptores de los certificados, y a las personas o entidades que contratan sus servicios de certificación regulados en esta Declaración de Prácticas de Certificación, las tarifas que en cada momento se encuentren en vigor.

9.1.1. Tarifas de emisión y renovación del certificado

Las tarifas de emisión y renovación de cada certificado están publicadas en el sitio web:

https://www.anf.ec

9.1.2. Tarifas de acceso al certificado

Servicio gratuito.

9.1.3. Revocación o tarifas de acceso a la información de estado

El servicio de revocación es gratuito.

El servicio de acceso a la información de estado de los certificados (de los certificados (OCSP, servicio de publicación de certificados revocados a partir de una fecha y hora) será de forma libre y gratuita.

9.1.4. Honorarios por otros servicios

9.1.4.1. Sellado de tiempo

Se aplican las tasas publicadas en sitio web: https://www.anf.ec

9.1.4.2. Retimbrado

Se aplican las tasas publicadas en sitio web: https://www.anf.ec

Certificado de verificación de firma

Se aplican las tasas publicadas en sitio web: https://www.anf.ec

Dispositivos de firma

Se aplican las tasas publicadas en sitio web: https://www.anf.ec

Otros servicios y soluciones de ANF AC

Se aplican las tasas publicadas en sitio web: https://www.anf.ec

9.1.5. Política de reembolso

Se aplican las tasas publicadas en sitio web: https://www.anf.ec

9.2. Responsabilidad financiera

9.2.1. Cobertura del seguro

De acuerdo con lo establecido en el artículo 30, letra h) de la Ley 67 de Comercio electrónico, firmas y mensajes de datos y con el detalle contenido en el Reglamento General de la Ley 67, la Entidad de Certificación deberá contar con una garantía de responsabilidad para cubrir daños y perjuicios que se ocasionaren por el incumplimiento de las obligaciones previstas en aquella Ley.

En ejecución de esa obligación legal, ANF AC ha suscrito seguro de responsabilidad civil en beneficio de la AGENCIA DE REGULACION Y CONTROL DE LAS TELECOMUNICACIONES ARCOTEL

Los datos relativos a la póliza son los siguientes:

- **Entidad Aseguradora:** SWEADEN COMPAÑIA DE SEGUROS S.A., Calle Sánchez de Ávila, núm. N3735, intersección con Av. Naciones Unidas, Edificio SWEADEN, Quito – Pichicha. R.U.C.: 1792107423001. Constituida en fecha 4 de septiembre de 2007 y registrada en la Superintendencia de Compañías, Valores y Seguros con el expediente 600827.
- **Núm. de póliza:** 0055018

9.2.2. Otros activos

Ninguna estipulación.

9.2.3. Seguro o cobertura de garantía para entidades finales

De acuerdo con el apartado 9.2.1.

9.3. Confidencialidad de la información

9.3.1. Alcance de la información confidencial

La siguiente información se considera confidencial y está protegida contra la divulgación utilizando un grado razonable de atención:

1. Claves privadas;
2. Los datos de activación utilizados para acceder a las claves privadas o para obtener acceso al sistema de CA;
3. Planes de continuidad del negocio, respuesta a incidentes, contingencia y recuperación de desastres.
4. Otras prácticas de seguridad utilizadas para proteger la confidencialidad, integridad o disponibilidad de la información;
5. Información mantenida por ANF AC como información privada de acuerdo con la Sección 9.4;
6. Registros de auditoría y registros de archivo; y

7. Registros de transacciones, registros de auditoría financiera y registros de seguimiento de auditoría externo o interno y cualquier informe de auditoría (con la excepción de la carta de un auditor que confirma la efectividad de los controles establecidos en esta DPC)

9.3.2. Información que no está dentro del alcance de la información confidencial

Cualquier información que no se enumera como confidencial se considera información pública. El certificado publicado y los datos de revocación se consideran información pública.

9.3.3. Responsabilidad de proteger la información confidencial

Los empleados, agentes y contratistas de ANF AC son responsables de proteger la información confidencial y tienen la obligación contractual de hacerlo. Los empleados reciben formación sobre cómo manejar la información confidencial.

9.4. Privacidad de la información personal

9.4.1. Política de Protección de Datos Personales

ANF AC dispone de una Política de Protección de Datos Personales publicada en: https://www.anf.ec
ANF AC realiza un tratamiento de datos de carácter personal de acuerdo con lo previsto en la Ley Orgánica de Protección de Datos Personales (LOPDP), publicada en el Registro Oficial Suplemento 459 de 26-may.-2021 y el Reglamento de la Ley Orgánica de Protección de Datos Personales (RGLOPDP), publicado en fecha 13-nov.-2023.

9.4.2. Información considerada privada

Se declara expresamente como información confidencial y no podrá ser divulgada a terceros, excepto en los casos en que la ley exija lo contrario:

- Cualquier información o dato, que, habiendo sido aportado por el suscriptor a la Entidad de Certificación o al Tercero Vinculado, no conste en el certificado electrónico.
- Toda información relativa a los parámetros de seguridad.
- Información o documentos que ANF AC haya clasificado como confidenciales.
- Registros de transacciones, incluyendo los registros completos y los registros de auditoría de las transacciones.
- Registros de auditoría interna y externa, creados y/o mantenidos por ANF AC o las Autoridades de Registro y sus auditores.

9.4.3. Información no considerada privada

La siguiente información es considerada no confidencial y de esta forma es reconocida por los afectados en los convenios vinculantes con ANF AC:

- Los certificados emitidos o en trámite de emisión.
- La vinculación de un suscriptor a un certificado emitido por ANF AC.
- La identidad del suscriptor del certificado, o del sujeto, así como cualquier otra circunstancia o dato personal de los mismos, en el supuesto de que sea significativa en función de la finalidad del certificado, y que conste registrada en el mismo.

- Los usos y límites económicos reseñados en el certificado, así como cualquier otra información contenida en el mismo.
- Los diferentes estados o situaciones del certificado y la fecha del inicio de cada uno de ellos, en concreto: pendiente de generación y/o entrega, válido, revocado, suspendido o caducado y el motivo que provocó el cambio de estado.
- Las Listas de Revocación de Certificados (CRL), así como las restantes informaciones de estado de revocación.
- La información contenida en el Servicio de Publicación de ANF AC clasificada como Pública.

9.4.4. Responsabilidad de proteger la información privada

ANF AC cumple en todo momento con la normativa vigente en materia de protección de datos. Ha adaptado sus procedimientos Ley Orgánica de Protección de Datos Personales (LOPDP) y a su Reglamento.

El documento de referencia a efectos de protección de datos y privacidad de ANF AC es la Política de Protección de Datos Personales, publicada en su sitio web https://www.anf.ec .

9.4.5. Aviso y consentimiento para usar la información privada

Los certificados serán objeto de publicación de acuerdo con lo establecido en el artículo 4.7 de la Resolución ARCOTEL-2024-01769, por la que se expide la "NORMA TÉCNICA PARA LA PRESTACIÓN DE LOS SERVICIOS DE INFORMACIÓN Y SERVICIOS RELACIONADOS DE LAS ENTIDADES DE CERTIFICACIÓN ACREDITADAS Y TERCEROS VINCULADOS".

Sobre el intercambio de datos de registro con el suscriptor o sujeto u otras partes que intervienen en la PKI, se toman medidas de seguridad que garanticen la confidencialidad y la integridad de la información.

9.4.6. Divulgación conforme al proceso judicial o administrativo

Como norma general ningún documento o registro perteneciente a ANF AC se envía a las autoridades judiciales o policiales, excepto cuando:

- El agente de la ley se identifica adecuadamente.
- Se proporcione una orden judicial debidamente redactada.
- La Autoridad de Certificación o de Registro tenga conocimiento de que los certificados emitidos, o alguno de los instrumentos pertenecientes a esta PKI, estén siendo utilizados para la comisión de un delito.

ANF AC divulgará la información confidencial únicamente en los supuestos legalmente previstos para ello.

En concreto, los registros que avalan la fiabilidad de los datos contenidos en el certificado serán divulgados en caso de ser requerido para ofrecer evidencia de la certificación en caso de un procedimiento judicial, incluso sin consentimiento del suscriptor del certificado.

9.4.7. Otras circunstancias de divulgación de información

Ninguna estipulación.

9.5. Derechos de propiedad intelectual

En los términos establecidos la Ley de Propiedad Intelectual, publicada en el Registro Oficial Suplemento 426 de 28 de diciembre de 2006, ANF AC es titular en exclusiva de todos los derechos relativos a los certificados electrónicos emitidos en el ámbito de su PKI en cualquiera de los tipos o modalidades de certificados, incluso las listas CRL y ARL de revocación de certificados.

Los identificadores de objeto (OID) utilizados son propiedad de ANF AC y han sido registrados en la Internet Assigned Number Authority (IANA) bajo la rama iso.org.dod.internet.private.enterprise 1.3.6.1.4.1-IANA-Registered Private Enterprises, habiéndose asignado el número:

- 1.3.6.1.4.1.37442

http://www.iana.org/assignments/enterprise-numbers

Queda prohibido, fuera del ámbito de la PKI de ANF AC, el uso total o parcial de cualquiera de los OID asignados a ANF AC.

- **Propiedad de los certificados e información de revocación:** La emisión y entrega de los certificados emitidos por ANF AC no presupone renuncia alguna sobre los derechos de propiedad intelectual que sobre ellos ostenta.

  ANF AC, salvo autorización expresa, prohíbe el almacenamiento de los datos de sus certificados en repositorios ajenos a la PKI de ANF AC, y especialmente cuando tenga como fin la prestación de servicios de información sobre el estado de vigencia o revocación.

  Los certificados y la información de estado sólo pueden ser utilizados para los fines de uso especificados en este documento.

- **Propiedad de los documentos relativos a la PKI:** ANF AC es propietaria de todos los documentos que publica en el ámbito de su PKI.

- **Propiedad de la información relativa a nombres:** El suscriptor conserva cualquier derecho, de existir éste, relativo a la marca, producto o nombre comercial contenido en el certificado. El suscriptor es el propietario del Nombre Distinguido del certificado.

- **Propiedad de claves:** Los pares de claves son propiedad de los suscriptores de los certificados. Cuando una clave se encuentra fraccionada en partes, todas las partes de la clave son propiedad del suscriptor.

9.6. Obligaciones

9.6.1. Obligaciones de la CA

Al emitir un Certificado, ANF AC otorga las garantías de certificado que se enumeran en este documento a los siguientes Beneficiarios del Certificado:

1. El Suscriptor que es parte en el contrato de suscripción o los Términos y Condiciones de uso para el Certificado;
2. Todos los proveedores de software de aplicación que hayan acordado incluir su certificado raíz en el software distribuido por dicho proveedor de software de aplicación; y
3. Todos los terceros que confían razonablemente en un Certificado válido.

ANF AC representa y garantiza a los Beneficiarios del certificado que, durante el período en que el Certificado es válido, ha cumplido con la ley vigente, las guías, estándares, requisitos aplicables y su Política de Certificación y / o Declaración de Prácticas de Certificación al emitir y administrar el certificado. ANF AC asume las siguientes obligaciones:

9.6.1.1. En la prestación del servicio

ANF AC presta sus servicios de certificación conforme con la presente Declaración de Prácticas de Certificación, responsabilizándose del cumplimiento de todas las obligaciones que le corresponden en su calidad de Entidad de Certificación y Servicios Relacionados Acreditada. Estas obligaciones de la Entidad de Certificación son las siguientes:

- No almacenar ni copiar los datos de creación de firma de la persona a la que haya prestado sus servicios.
- Mantener un sistema en el que se indicarán los certificados expedidos y si están vigentes o si su vigencia ha sido suspendida o extinguida.
- Conservar durante todo el periodo de vigencia de la acreditación toda la información y documentación relativa a los certificados emitidos y a las declaraciones de prácticas de certificación vigentes en cada momento. .
- Comprueba que el firmante está en posesión de los datos de creación de firma correspondientes a los de verificación que constan en el certificado.

9.6.1.2. De operación fiable

ANF AC garantiza:

- Que la identidad contenida en el certificado se corresponde de forma unívoca con la clave pública contenida en el mismo.
- Se permite la utilización de un servicio rápido y seguro de consulta de validez de los certificados de acuerdo con lo establecido en esta DPC. Este servicio está disponible de forma permanente 24x7x365.
- El cumplimiento de los requisitos técnicos y de personal exigidos por la legislación vigente en materia de firma electrónica:
    1. Demostrar la fiabilidad necesaria para prestar servicios de certificación.
    2. Garantizar que pueda determinarse con precisión la fecha y hora en las que se expidió un certificado o se extinguió o suspendió su vigencia.

3. Emplear el personal con la cualificación, conocimientos y experiencia necesarios para la prestación de los servicios de certificación ofrecidos y los procedimientos de seguridad y gestión adecuados en el ámbito de la firma electrónica.

4. Utilizar sistemas y productos fiables que estén protegidos contra toda alteración y que garanticen la seguridad técnica y, en su caso, criptográfica de los procesos de certificación a los que sirven de soporte, de acuerdo con la Política de Seguridad.

5. Tomar medidas contra la falsificación de certificados y garantizar la confidencialidad en el proceso de generación de acuerdo con lo indicado en el apartado 6 y realizar su entrega por un procedimiento seguro al firmante.

6. Utilizar sistemas fiables para almacenar certificados cualificados que permitan comprobar su autenticación e impedir que personas no autorizadas alteren los datos, que restrinjan su accesibilidad en los supuestos o a las personas que el firmante haya indicado y que permitan detectar cualquier cambio que afecte a estas condiciones de seguridad.

- La correcta gestión de su seguridad, gracias a la implementación de un Sistema de Gestión de la Seguridad de la Información de acuerdo a los principios establecidos por la ISO/IEC 27001 y que incluye, entre otras, las siguientes medidas:

    1. Realizar de forma periódica comprobaciones regulares de la seguridad, con el fin de verificar la conformidad con los estándares establecidos.

    2. Llevar a cabo una completa gestión de los sucesos de seguridad, con el fin de garantizar su detección, resolución y optimización.

    3. Mantener los contactos y relaciones apropiados con grupos de especial interés en materia de seguridad, como especialistas, foros de seguridad y asociaciones profesionales relacionadas con la seguridad de la información.

    4. Planificar adecuadamente el mantenimiento y evolución de los sistemas, con el fin de garantizar en todo momento un rendimiento adecuado y un servicio que cumpla con todas las garantías las expectativas de los usuarios y clientes.

9.6.1.3. De identificación

ANF AC identifica al suscriptor del certificado de acuerdo con la normativa vigente y la presente Declaración de Prácticas de Certificación.

9.6.1.4. De información a usuarios

Antes de la emisión y entrega del certificado al suscriptor, ANF AC o el Tercero Vinculado, en nombre y representación de ANF AC, le informa de los términos y condiciones relativos al uso del certificado, de su precio, de sus limitaciones de uso y le facilita documentación relativa a los derechos y obligaciones inherentes al uso de los servicios de certificación de ANF AC, en especial a la custodia y privacidad de los instrumentos de firma y datos de activación de firma electrónica. Los términos y condiciones de la contratación pueden ser descargadas por tercera parte accediendo a la página web de ANF AC.

Este requisito es cumplido mediante la formalización del correspondiente contrato de solicitud de certificado y prestación de servicios.

ANF AC asume la obligación de comunicar a los firmantes el cese de sus actividades de prestación de servicios de certificación con dos meses de antelación e informar, en su caso, sobre las características de la Entidad de Certificación a la que se propone la transferencia de la gestión de los certificados. Las comunicaciones a los signatarios se efectúan conforme a lo previsto en el presente documento.

ANF AC dispone de un plan de cese de su actividad en el que se especifican las condiciones en las que se realizaría.

Toda esta información pública relativa a los certificados está a disposición del público en general en los repositorios de ANF AC indicados en esta DPC.

9.6.1.5. Relativa a los programas de verificación

ANF AC ofrece mecanismos de verificación de la validez de los certificados y firmas electrónicas, mediante los sistemas descritos en el presente documento.

9.6.1.6. Relativa a la regulación jurídica del servicio de certificación

ANF AC asume todas las obligaciones incorporadas directamente en el certificado o incorporadas por referencia. La incorporación por referencia se logra incluyendo en el certificado un identificador de objeto u otra forma de enlace a un documento.

El instrumento jurídico que vincula a ANF AC y al suscriptor o sujeto y al tercero que confía en el certificado está en lenguaje escrito y comprensible, teniendo los siguientes contenidos mínimos:

- Indicación que posibilita al suscriptor conocer y posibilitar el cumplimiento de sus obligaciones y derechos.
- Indicación de la Declaración de Prácticas de Certificación aplicable, con especificación, en su caso, de que los certificados se expiden con la necesidad de empleo de dispositivo seguro de creación de firma o descifrado de mensajes homologado por ANF AC.
- Cláusulas relativas a la emisión, revocación, y renovación de certificados.
- Manifestación de que la información contenida en el certificado es correcta, excepto notificación en contra por el suscriptor.
- Consentimiento para el almacenamiento de la información empleada para el registro del suscriptor, para la provisión de un dispositivo criptográfico y para la cesión de dicha información a terceros, en caso de terminación de operaciones de ANF AC sin revocación de certificados vigentes.
- Límites de uso del certificado.
- Información sobre cómo validar un certificado, incluyendo el requisito de comprobar el estado del certificado, y las condiciones en las cuales se puede confiar razonablemente en el certificado.
- Limitaciones de responsabilidad aplicables, incluyendo los usos por los cuales ANF AC acepta o excluye su responsabilidad.
- Periodo de archivo de información de solicitud de certificados.

- Procedimientos aplicables de resolución de disputas.
- Ley aplicable y jurisdicción competente.
- Forma en la que se garantiza la responsabilidad patrimonial de ANF AC.

9.6.2. Obligaciones de los Terceros Vinculados

En su art. 33 la Ley 67 de Comercio Electrónico, Firmas y Mensajes de Datos reconoce la posibilidad de que las entidades de certificación puedan colaborar con terceros en la prestación de sus servicios, pero no obstante establece que la responsabilidad única de los servicios de certificación recae completamente sobre la Entidad de Certificación. Los Terceros Vinculados son responsables ante ANF AC por los daños que causen en el ejercicio de sus funciones, de acuerdo con las obligaciones establecidas en el correspondiente convenio, y con las seguidamente enunciadas:

- Transcribir con exactitud, en los formularios de solicitud del dispositivo AR Manager, la información recogida de los documentos originales aportados por los suscriptores.
- Admitir únicamente documentación original en el proceso de identificación, obteniendo copia de la documentación aportada por los suscriptores. Dicha documentación será remitida a la autoridad de certificación para su guarda y custodia o conservada por el Tercero Vinculado a disposición de la Entidad de Certifiación.
- No facilitar a terceros copia de la documentación obtenida de los suscriptores, ni información alguna de los mismos o los sujetos.
- Custodiar el dispositivo AR Manager, no permitiendo su uso o la revisión del mismo por terceros no autorizados y, en caso de pérdida, comunicar inmediatamente a ANF AC.
- Aplicar las tasas oficiales sin efectuar incremento ni cargo alguno por ningún otro concepto que no sean los estipulados por ANF AC.
- En caso de cese en la actividad como Tercero Vinculado, proceder a la devolución del dispositivo AR Manager, así como a cuanta documentación o material obre en su poder derivado de la actividad realizada como Tercero Vinculado.
- Comunicar cualquier reclamación judicial o extrajudicial que se produzca en el ámbito de su actividad como Tercero Vinculado.
- En relación a la información contenida en el certificado o características personales que le capacitaron en su momento para obtener la acreditación como Tercero Vincluado, debe informar de cualquier cambio que se produzca en sus circunstancias personales.
- Proteger y custodiar personalmente las Claves Privadas del Tercero Vinculado y la contraseña de activación contra peligro de usurpación o uso indebido. Ante cualquier sospecha de quebranto de seguridad debe comunicarlo inmediatamente y proceder a su revocación.
- Ser diligente en la atención de los suscriptores, facilitando, a ser posible, información de los documentos originales que les serán requeridos y evitando esperas innecesarias.
- No utilizar las copias que el suscriptor acompañe a la documentación original. Cualquier copia en papel o digitalizada será obtenida directamente por el Tercero Vinculado.

- Comunicar de forma diligente a ANF AC la existencia de solicitudes de emisión de certificados, en especial aquellas que ha rechazado.
- No mediar en la generación de los datos de creación de firma de los usuarios, ni permitir ser informado del PIN de activación elegido por el suscriptor.
- Almacenar, de forma segura y permanente, copia de la documentación aportada por el usuario para realizar su petición, así como de la documentación generada por el AR Manager, durante el proceso de petición, registro o revocación.
- Colaborar con las auditorías dirigidas por ANF AC para validar la renovación de sus propias claves.
- Respetar la privacidad de los suscriptores y titulares de certificados conforme a lo establecido en la Ley Orgánica de Protección de Datos de Carácter Personales y demás normativa aplicable.

9.6.3. Obligaciones de los suscriptores y responsables de los certificados

Las responsabilidades de los titulares de los certificados están establecidas en las Políticas de Certificación correspondientes. Además, de forma general y complementaria se establece que:

- Los suscriptores de certificados de ANF AC se responsabilizan de cumplir todas las obligaciones derivadas del presente documento, Política de Firma Electrónica, Políticas de Certificación y Contrato de Suscripción y Términos y Condiciones, limitando y adecuando el uso del certificado y de los sistemas de firma electrónica contemplados en el ámbito de esta PKI a propósitos lícitos y acordes con una honesta y leal actuación con toda la comunidad: ANF AC, Terceros Vinculados, usuarios y terceros que confían. La siguiente relación es meramente enunciativa y no limitativa.

El suscriptor se compromete a:

- Asegurarse de que toda la información contenida en el Certificado es cierta.
- Asegurarse de que la documentación aportada en la tramitación de la solicitud de certificado es veraz y auténtica.
- En el momento de recibir su certificado electrónico, comprobar urgentemente la correspondencia del mismo con la petición formulada. Para ello, emplea la opción de comprobación de certificados que incluye el dispositivo de generación de datos de creación de firma. En caso de que la comprobación resulte negativa, comunicará el hecho de forma inmediata a ANF AC.
- Utilizar el certificado respetando las restricciones que le vienen impuestas según su Política de Certificación y la Política de Firma Electrónica.
- En caso de que el certificado reseñe “Declaración del Emisor, Atributos y Limitaciones de uso”, deberá atenerse a lo allí indicado.
- Custodiar, de forma diligente, el contenedor de los datos de creación de firma y la clave secreta de activación, así como nombre de usuario y contraseña secreta de acceso al registro general.
- Emplear exclusivamente dispositivos de ANF AC, tanto para el almacenamiento de los datos de generación de firma, como para la creación de firmas electrónicas, como su posterior verificación.

- Mantener actualizados los dispositivos criptográficos de ANF AC, siguiendo en su instalación y mantenimiento las instrucciones que a tal efecto le facilite ANF AC, y garantizar que los dispositivos no han sido desatendidos de la protección que facilita ANF AC.
- Previo a la creación de una firma electrónica empleando un dispositivo criptográfico de ANF AC, verificar los atributos de firma que serán incluidos en la firma electrónica, y sólo activar el proceso de firma si está conforme con todos ellos.
- Aceptar todas las firmas electrónicas vinculadas al certificado del que es titular, siempre que hayan sido creadas empleando un certificado vigente.

La imprescindible activación de los datos de creación de firma, por parte del signatario mediante el empleo de su clave secreta, presupone:

- El consentimiento pleno de creación de la firma electrónica, y la aceptación de la Política de Firma Electrónica asociada a esa firma.
- La solicitud de revocación del Certificado cuando se vea comprometida la seguridad de los datos de creación de firma o la clave secreta de activación, o cuando sus datos personales hayan sufrido alguna modificación.
- En caso de revocación del Certificado, la obligación del suscriptor de cesar en su uso.

Los usuarios garantizan que las denominaciones, nombre o dominios reseñados en el formulario de solicitud y en el contrato de prestación de servicios no infringen los derechos de terceros en ninguna jurisdicción con respecto a derechos de propiedad industrial y marca, que no emplearán el dominio y nombre distintivo para propósitos ilícitos; entre ellos, competencia desleal, suplantación, usurpación y actos de confusión en general.

Los suscriptores y, en general, los usuarios de certificados, indemnizarán a ANF AC por los daños que le pueda causar en la realización de estas actividades. Asimismo, se comprometen a:

- Suministrar a los Terceros Vinculados documentación original e información que consideren exacta y completa. Así como a notificar cualquier modificación que sobre la misma se produzca.
- Abonar las tasas de los servicios que le sean prestados por parte de la AC, o por parte del Tercero Vinculado.
- No tramitar solicitud de certificado alguno en caso de haber mantenido algún tipo de conflicto de intereses con ANF AC o miembros de la Junta Rectora.
- Realizar la solicitud de certificado bajo el principio de buena fe, y con el único interés de hacer uso del mismo para los fines que comúnmente son aceptados.
- Y en general, a todas las derivadas de la la Ley 67 de Comercio Electrónico, Firmas y Mensajes de Datos.

9.6.4. Obligaciones de los terceros que confían

Tiene la consideración de receptor el tercero de buena fe que confía en el fichero electrónico que está firmado electrónicamente por un usuario de ANF AC y que, además de depositar la confianza en esa firma electrónica, cumple con las siguientes obligaciones:

- Verificar la firma utilizando un dispositivo de verificación de firma electrónica de ANF AC.
- Comprobar el estado de vigencia del certificado utilizando uno de los medios autorizados por este QTSP.

- Actuar de forma diligente. Se considerará que la actuación ha sido negligente si incurre en alguno de los supuestos contemplados en el art. 17 de la la Ley 67 de Comercio Electrónico, Firmas y Mensajes de Datos.
- Valorar la adecuación del certificado asociado a la firma electrónica, de acuerdo con: el tipo de certificado, la declaración del emisor, las limitaciones de uso que en el mismo se reseñan, y las declaradas en esta DPC y la Política de Certificación a la que se somete.
- Solicitar el asesoramiento de la "Oficina de Atención al Cliente" de ANF AC en caso de duda.

ANF AC pone a disposición de los terceros que confían las listas de revocación de certificados. El tercero puede acceder a esta información con el único uso y fin personal de verificar el estado de vigencia de un certificado de su interés, en ningún caso para la prestación de servicios a terceros.

Los receptores que no cumplan los requisitos indicados, no podrán ser considerados de buena fe.

9.6.5. Obligaciones de otros participantes

Ninguna estipulación.

9.7. Exención de garantías

ANF AC puede rechazar toda garantía de servicio que no se encuentre vinculada a las obligaciones establecidas por la vigente Ley 67 de Comercio Electrónico, Firmas y Mensajes de Datos.

9.8. Limitaciones de responsabilidad

9.8.1. Limitación de responsabilidad con el suscriptor

- ANF AC no asume responsabilidades derivadas de denegaciones de servicio, salvo en aquellos casos en los que el contrato de suscripción establezca una penalización al respecto.
- ANF AC no asume responsabilidad por las transacciones realizadas por sus suscriptores mediante el uso de sus certificados.
- ANF AC no asume responsabilidad cuando el titular hace uso de los certificados utilizando instrumentos que no están homologados por ANF AC.
- ANF AC se acoge a otras exenciones establecidas en la Política de Certificación correspondiente al tipo de certificado en cuestión.
- A excepción de lo establecido en este documento, ANF AC no asume ningún otro compromiso ni brinda ninguna otra garantía, así como tampoco asume ninguna otra responsabilidad ante titulares de certificados, sus representantes legales y/o sus responsables de certificados.

9.8.2. Limitación de responsabilidad con el tercero que confía

- ANF AC no asume responsabilidad cuando el tercero que confía no materializa su obligación de verificar el estado del certificado, utilizando los instrumentos de verificación de ANF AC.

- ANF AC se acoge a otras exenciones establecidas en la Política de Certificación correspondiente al tipo de certificado en cuestión.
- A excepción de lo establecido en este documento, ANF AC no asume ningún otro compromiso ni brinda ninguna otra garantía, así como tampoco asume ninguna otra responsabilidad ante terceros que confían.

9.9. Responsabilidad Civil

ANF AC, en este documento, en las Políticas de Certificación y en los convenios que le vinculan con el suscriptor, con sus Terceros Vinculados y los Terceros que Confían, incluye cláusulas de indemnidad en caso de infracción de sus obligaciones o de la legislación aplicable.

ANF AC hace constar que en los certificados emitidos el límite asumido por la CA queda establecido en el propio certificado, concretamente en la Extensión "QcStatements" en el campo "QcLimitValue" OID 0.4.0.37442.1.2. y en la extensión propietaria OID 1.3.6.4.1. 37442.41.1.

Si no se fija cantidad alguna, se deberá interpretar que la CA no asume el uso de ese certificado para transacciones que conlleven riesgo financiero alguno, y por lo tanto el límite de indemnización es cero.

9.9.1. De la CA

ANF AC responderá de aquellos perjuicios que vengan derivados, con carácter general:

- De un incumplimiento de las obligaciones contenidas en la Ley 67 de Comercio Electrónico, Firmas y Mensajes de Datos y normativa de desarrollo, en la presente DPC y en las Políticas de Certificación correspondientes.

Y de forma específica:

- Según lo previsto en el artículo 30 de la Ley 67 de Comercio Electrónico, Firmas y Mensajes de Datos, ANF AC responderá por los daños y perjuicios que cause a cualquier persona por la falta o retraso en la inclusión en el servicio de consulta sobre la vigencia de los certificados o de la extinción o suspensión de la vigencia de los certificados.
- ANF AC asume toda la responsabilidad frente a terceros por la actuación de las personas en las que delegue funciones necesarias para la prestación de servicios de certificación.
- La CA deberá defender, indemnizar y mantener indemne a cualquier proveedor de software de aplicaciones por reclamaciones, daños y pérdidas sufridas por dicho proveedor de software de aplicaciones en relación con un certificado expedido por la CA, independientemente de la causa. Lo anterior no será de aplicación en reclamaciones de daños y perjuicios.

En cualquier caso, se exceptúan en los siguientes supuestos, de **carácter general:**

- ANF AC no será responsable de ningún daño directo e indirecto, especial, incidental, emergente, de cualquier lucro cesante, pérdida de datos, daños punitivos, fuesen o no previsibles, surgidos en relación con el uso, entrega, licencia, funcionamiento o no funcionamiento de los certificados, las firmas electrónicas, o cualquier otra transacción o servicio ofrecido o contemplado en la Declaración de Prácticas de Certificación en caso de uso indebido, o cuando se utilicen en transacciones que conlleven un riesgo superior al expresado en el límite de indemnización de expresado por la CA.

- En todos los supuestos previstos en el artículo de la Ley 67 de Comercio Electrónico, Firmas y Mensajes de Datos.
- ANF AC no asume ningún otro compromiso o responsabilidad que los detallados en esta Declaración de Prácticas de Certificación.

De forma específica con los **suscriptores y los responsables de los certificados:**

- Cuando incumplan las obligaciones contenidas en la Ley 67 de Comercio Electrónico, Firmas y Mensajes de Datos y normativa de desarrollo, en la presente DPC y en las Políticas de Certificación correspondientes. En especial las obligaciones reseñadas en el apartado 9.6.3 de esta DPC.

Y de forma específica con los **terceros que confían**:

- Cuando incumplan las obligaciones contenidas en la Ley 67 de Comercio Electrónico, Firmas y Mensajes de Datos y normativa de desarrollo, en la presente DPC y en las Políticas de Certificación correspondientes. En especial las obligaciones reseñadas en el apartado 9.6.4 de esta DPC.

9.9.2. Del suscriptor

El suscriptor es responsable de todas las comunicaciones electrónicas autenticadas y documentos autenticados, en los que se ha empleado una firma digital generada con su clave privada, y el certificado ha sido válidamente confirmado a través de los servicios de verificación de ANF AC.

Dentro del periodo de vigencia del certificado, o en tanto en cuanto no conste la revocación del certificado en los registros de ANF AC, la responsabilidad que pudiera derivarse del uso no autorizado y/o indebido de los Certificados, corresponderá, en todo caso, al suscriptor.

Con la aceptación del Certificado, el suscriptor se obliga a mantener indemne y, en su caso, a indemnizar a ANF AC, a sus Terceros Vinculados y a Terceros que confían de cualquier acto u omisión que provoque daños, pérdidas, deudas, gastos procesales o de cualquier tipo, incluyendo los honorarios profesionales, en los que se puedan incurrir. En especial cuando provenga:

- del incumplimiento de los términos previstos en solicitud de certificados y contratación de servicios de certificación que lo vincula con ANF AC;
- del uso de los Certificados en operaciones en las que no se ha respetado el límite de uso o que están prohibidas, conforme a lo expresado en esta DPC y Políticas de Certificación que correspondan;
- de falsedad o el error intencionado cometido por el suscriptor;
- de toda omisión de un hecho fundamental en los certificados realizada negligentemente o con la intención de engañar;
- del incumplimiento del deber de custodia de las claves privadas, y de tomar aquellas precauciones que sean razonables para prevenir la pérdida, revelación, alteración o uso no autorizado de las claves privadas;
- del incumplimiento del deber de mantener la confidencialidad de los datos de creación de firma y protegerlos de todo acceso o revelación;
- del incumplimiento del deber de solicitar la suspensión o revocación del certificado en caso de duda en cuanto al mantenimiento de la confidencialidad de sus datos de creación de firma;

- del incumplimiento del deber de abstenerse de utilizar los datos de creación de firma desde el momento en que haya expirado el período de validez del certificado o el prestador de servicios le notifique su pérdida de vigencia;
- del incumplimiento del deber de comunicar sin demora cualquier modificación de las circunstancias reflejadas en el certificado.

9.9.3. De los Terceros que confían

El tercero que confíe en un certificado no vigente o una firma digital que no ha sido verificada con los dispositivos que ANF AC ha desarrollado y homologado con tal fin, asume todos los riesgos relacionados con la misma y no podrá exigir responsabilidad alguna a ANF AC, a los Terceros Vinculados, o a los suscriptores por cualquier concepto derivado de su confianza en tales certificados y firmas.

En este sentido, ANF AC tampoco será responsable por los daños y perjuicios ocasionados al suscriptor o a terceros que confían, si el destinatario de los documentos firmados electrónicamente incumple con alguna de las obligaciones establecidas en la Ley 67 de Comercio Electrónico, Firmas y Mensajes de Datos y normativa de desarrollo, en la presente DPC, en las Políticas de Certificación a las que se somete el certificado electrónico empleado en la transacción, y en especial por incumplimiento de las responsabilidades reseñadas en el apartado 9.6.4 de este documento.

9.9.4. De los Terceros Vinculados

En el supuesto de que el Tercero Vinculado de ANF AC incumpla las obligaciones contenidas en la Ley 67 de Comercio Electrónico, Firmas y Mensajes de Datos y normativa de desarrollo, en la presente DPC, en las Políticas de Certificación correspondientes a los trámites de certificación en los que interviene, y en los términos que establecen el convenio que formaliza su actividad como Tercero Vinculado, será responsable frente a ANF AC por los daños causados en el ejercicio de las funciones que asuma.

Los Terceros Vinculados disponen de suficientes recursos para mantener sus operaciones y realizar sus tareas. Los Terceros Vinculados son razonablemente capaces de asumir el riesgo de responsabilidad civil hacia suscriptores y terceros que confían.

9.10. Periodo de validez

9.10.1. Periodo de validez

Esta Declaración de Prácticas de Certificación y todas las Políticas de Certificación y Firma de ANF AC entran en vigor el día reseñado en el campo “Fecha de publicación” del apartado 1.2.

9.10.2. Derogación

Será derogada el día que entre en vigor una nueva versión de dicha política de ANF AC.

9.10.3. Efecto de la derogación y supervivencia

Las obligaciones, derechos y restricciones establecidas en esta Declaración de Prácticas de Certificación, y en las respectivas Políticas de Certificación y Firma Electrónica, nacidas durante su periodo de vigencia, perdurarán tras su derogación.

9.11. Avisos individuales y comunicaciones con los participantes

ANF AC se compromete a tener plenamente operativo un servicio gratuito de atención de usuarios y receptores.

9.11.1. Cometido de la Oficina

Este servicio atenderá cuantas consultas comerciales, jurídicas y técnicas estén relacionadas con:

- La actual legislación vigente sobre certificación y firma electrónica.
- Esta DPC, Políticas de Certificación y documento de solicitud de certificados.
- La instalación y utilización de los dispositivos relacionados con la firma electrónica.
- La instalación y utilización del software homologado.
- La generación y uso de los contenedores homologados y, en general, todo lo relacionado con la prestación de servicios de certificación que esta AC realiza.
- Consultas generales sobre los conceptos básicos de Infraestructura de Clave Pública, certificados electrónicos y, firma electrónica.

Asimismo, realizará en nombre del usuario o de la persona a la que éste representa, las distintas operaciones que esta DPC, y Políticas de Certificación le encomienden.

9.11.2. Procedimiento de Consulta

Las consultas se realizarán mediante correo electrónico dirigido a: info@anf.ec

En ellas se reseñará el identificador del usuario que consulta o, en caso de ser receptor, el identificador de la firma recibida. Las consultas así realizadas son contestadas por este mismo medio a la dirección electrónica del remitente.

También está disponible un servicio de atención personal mediante llamada telefónica al +593 02 3826877.

9.11.3. Procedimiento de Reclamación

En caso de desear presentar una reclamación, esta entidad prestadora de servicios de certificación, cuenta con un formulario en

https://www.anf.ec

Toda notificación, demanda, solicitud o cualquier otra comunicación requerida bajo las prácticas descritas en esta DPC se realizará mediante documento o mensaje electrónico firmado electrónicamente de conformidad con esta última o por escrito mediante correo certificado dirigido a cualquiera de las direcciones contenidas en el punto 1.5.1 de esta Entidad de Certificación. Las comunicaciones electrónicas se harán efectivas una vez que las reciba el destinatario al que van dirigidas.

También es posible dirigirse personalmente ante la Oficina de Atención al Cliente.

ANF AC contestará por escrito a la reclamación formulada en un tiempo no superior a 15 días hábiles. En caso de que la respuesta no sea satisfactoria, se seguirá con lo reseñado en el apartado “Procedimientos de resolución de disputas” de este documento.

9.11.4. Procedimiento de Identificación

Aquellos que se personen ante la Oficina de Atención al Cliente deben identificarse fehacientemente mediante cédula de identidad o ciudadanía, documento nacional de identidad o pasaporte original. Aquellas personas que actúen en representación de terceros deberán presentar apoderamiento suficiente.

9.12. Enmiendas

9.12.1. Procedimiento para enmiendas

ANF AC podrá realizar modificaciones de sus documentos y políticas sin necesidad de publicar un nuevo documento y, por lo tanto, aplicar un cambio de versión siempre y cuando no sean cambios materiales, como, por ejemplo:

- Correcciones de errores tipográficos en el documento
- Modificaciones de direcciones URL
- Cambios en la información de contacto.

Cualquier modificación no contemplada en el apartado anterior, conlleva la publicación de un nuevo documento y su cambio de versión.

9.12.2. Periodo y mecanismo de notificación

Se sigue lo establecido en el Apartado 2 de este documento

9.12.3. Circunstancias bajo las cuales se debe cambiar el OID

El identificador de los documentos de ANF AC solo será cambiado si se producen cambios sustanciales que afectan a su aplicabilidad.

9.13. Disposiciones de resolución de disputas

9.13.1. Procedimiento extrajudicial

ANF AC se esforzará en resolver de forma amistosa los conflictos que surjan con terceras partes por el ejercicio de su actividad, sólo recurriendo al procedimiento previsto en el apartado siguiente, cuando el acuerdo entre las partes resulte inalcanzable.

9.13.2. Procedimiento judicial

ANF AC se somete voluntariamente, para la solución de cualquier cuestión litigiosa que pudiera surgir por el ejercicio de su actividad, al arbitraje institucional del Tribunal Arbitral del Consejo Empresarial de la Distribución (TACED), al que se le encarga la designa del Árbitro – que será único – y la administración del arbitraje – que será de equidad – con arreglo a su Reglamento, obligándose desde ahora, al cumplimiento de la decisión arbitral.

Si por alguna causa no fuera posible dirimir la controversia mediante el procedimiento arbitral reseñado en el punto anterior, las Partes, con renuncia a cualquier otro fuero que pudiera corresponderles, se someten para la resolución de cualquier conflicto que pudiera surgir entre las mismas, a los tribunales de la ciudad de Quito, con renuncia a su fuero propio si fuera distinto.

9.14. Ley aplicable

La normativa aplicable al presente documento, así como a las distintas CP, y a las operaciones que derivan de ellas, es la siguiente:

- 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.
- Reglamento General de la Ley de Comercio Electrónico, Firmas y Mensajes de Datos, publicado en el Registro Oficial Suplemento No. 735 de 31 de diciembre de 2002.
- Decreto núm. 1356, de 29 de septiembre de 2008, de Reforma del Reglamento General de la Ley de Comercio Electrónico, Firmas y Mensajes de Datos.
- Resolución ARCOTEL-2024-0176, de fecha 16 de agosto de 2024, por la que se expide la "NORMA TÉCNICA PARA LA PRESTACIÓN DE LOS SERVICIOS DE INFORMACIÓN Y SERVICIOS RELACIONADOS DE LAS ENTIDADES DE CERTIFICACIÓN ACREDITADAS Y TERCEROS VINCULADOS".
- Ley Orgánica de Protección de Datos Personales (LOPDP), publicada en el Registro Oficial Suplemento 459 de 26-may.-2021.
- Reglamento de la Ley Orgánica de Protección de Datos Personales (RGLOPDP), publicado en fecha 13-nov.-2023.
- Ley Orgánica de Defensa del Consumidor, publicada en el Registro Oficial. Suplemento No. 116 del 10 de julio del 2000.
- Reglamento General de la Ley Orgánica de Defensa del Consumidor.
- Cualquier otra disposición que contemple aspectos relaciones con la firma electrónica, seguridad de la información, protección de datos personales y privacidad.

9.15. Cumplimiento de la legislación aplicable

ANF AC manifiesta el cumplimiento de la legislación aplicable reseñada en el punto anterior.

En concreto, con carácter enunciativo, que no limitativo, ANF AC deja constancia de cumplimiento de las siguientes obligaciones:

- Remitir a la Agencia de Regulación y Control de las Telecomunicaciones ARCOTEL, con una periodicidad trimestral desagregado de manera mensual, dentro de los primeros quince (15) días del trimestre siguiente al del objeto del reporte, y conforme a los formularios que ésta establezca para el efecto, la siguiente información:
    - Número de certificados emitidos, vigentes revocados y suspendidos, por tipo.
    - Facturación total del mes.
- Suministrar la información que requ era la ARCOTEL, así como a las entidades administrativas competentes o judiciales en relación con las firmas electrónicas y certificados emitidos; y, en general sobre cualquier Mensaje

de Datos que se encuentre bajo su custodia y administración.

- Informar a la Agencia de Regulación y Control de las Telecomunicaciones, en el término máximo de dos (2) días, la ocurrencia de cualquier evento que comprometa la disponibilidad y la seguridad en la prestación de los servicios de certificación de información y servicios relacionados con la firma electrónica.

Esta DPC debe interpretarse con arreglo a la legislación vigente, sus disposiciones de desarrollo y la legislación específica que afecta a sus servicios, especialmente en materia de protección de datos personales y legislación sobre protección de los consumidores y usuarios.

Las discrepancias de interpretación se dirimirán ante los Juzgados y Tribunales de la ciudad de Quito.

9.16. Otras disposiciones

9.16.1. Acuerdo íntegro y notificación

Ninguno de los términos de esta Declaración de Prácticas de Certificación que afecte directamente a los derechos y obligaciones de ANF AC y que no afecte al resto de las partes, puede ser corregido, renunciado, suplementado, modificado o eliminado si no es mediante documento escrito autenticado de ANF AC, que no supone en ningún caso novación extintiva, sino meramente modificativa, y no afecta al resto de derechos y obligaciones de las restantes partes.

Las notificaciones deben de ser dirigidas a:

ANF Autoridad de Certificación Ecuador C.A.

Dirección: Av. 12 de Octubre N24-739 y Av. Colon - Ed. Torre Boreal

170143 - Quito (Ecuador)

Las notificaciones pueden realizarse de forma personal o mediante notificación por escrito, en cualquier caso, se debe garantizar de forma fehaciente la identidad de la persona que interviene en la comunicación. En caso de representar a un tercero, además tiene que acreditar de forma suficiente su capacidad de representación.

9.16.2. Asignación

Corresponde a los terceros que confían en los certificados emitidos por ANF AC, y en las firmas/sellos generados con ellos, o en otros servicios de confianza prestados por ANF AC, proceder a la verificación de los mismos con carácter previo a otorgar su confianza, en especial comprobando el estado de vigencia del certificado en el momento de su uso. Para llevar a cabo esta obligación, se deberá utilizar un servicio cualificado de validación.

Los servicios de consulta en línea OCSP que permiten determinar el estado de vigencia de un certificado, están disponibles gratuitamente a los terceros que confían, y plataformas multi validación con las que ANF AC haya suscripto el correspondiente acuerdo de colaboración. Está prohibido el acceso para prestar servicios de intermediación de validación, este acceso tendrá un costo de un 1 dólar por consulta.

9.16.3. Divisibilidad

Si alguno de los apartados de este documento o de las Políticas es considerado nulo o legalmente inexigible, se considerará por no puesto, perdurando el resto de obligaciones, derechos y restricciones establecidos en este documento.

La cláusula inválida o incompleta podrá ser sustituida por otra equivalente y válida por acuerdo de las partes.

Las normas contenidas en las secciones: Obligaciones, Responsabilidad Civil y Confidencialidad, permanecerán en vigor tras la finalización de la vida de esta Declaración de Prácticas de Certificación

Según establecen los *Baseline Requirements* de CA/B Forum, en caso de contradicción entre dichos requisitos y una ley, reglamento u orden del gobierno (en adelante, "Ley") de cualquier jurisdicción en la que ANF AC opera o emite certificados, ANF AC podrá modificar cualquier requisito en conflicto en la medida mínima necesaria para hacer el requisito vigente y legal en la jurisdicción. Esto se aplica sólo a las operaciones o emisiones de certificados que están sujetos a esa Ley. En tal caso, ANF AC incluirá inmediatamente (y antes de emitir un certificado según el requisito modificado) en esta sección 9.16.3 de la DPC una referencia detallada a la Ley que requiere una modificación de estos Requisitos en esta sección, y la modificación específica a estos requisitos implementados por ANF AC.

Antes de emitir un certificado según el requisito modificado, ANF AC notificará a CA/Browser Forum la información relevante recién agregada a su DPC enviando un mensaje a questions@cabforum.org y recibiendo la confirmación de que ha sido publicado en la Lista de Correo Pública y está indexado en los Archivos de Correo Público disponibles en https://cabforum.org/pipermail/public/ (o cualquier otra dirección de correo electrónico y enlaces que el Foro pueda designar). Esto se realizará en un plazo máximo de 90 días.

Cualquier modificación a la práctica de ANF AC habilitada en esta sección será descontinuada si la Ley ya no se aplica, y si los Baseline Requirements se modifican para que sea posible cumplir con ellos y la Ley simultáneamente.

9.16.4. Cumplimiento (honorarios de abogados y renuncia de derechos)

ANF AC puede solicitar una indemnización y honorarios de abogados de una parte por daños, pérdidas y gastos relacionados con la conducta de dicha parte.

El hecho de que ANF AC no haga cumplir una disposición de esta DPC no elimina el derecho de ANF AC de hacer cumplir las mismas disposiciones más adelante o el derecho de hacer cumplir cualquier otra disposición de esta DPC.

Para ser efectiva, cualquier renuncia debe constar por escrito y firmada por ANF AC.

9.16.5. Fuerza mayor

ANF AC no es responsable de un retraso o incumplimiento de cumplir con una obligación en virtud de esta DPC o cualquier Política de Certificación en la medida en que dicho retraso o incumplimiento sea causado por una circunstancia fuera del control razonable de ANF AC. El funcionamiento de Internet está fuera del control razonable de ANF AC.

9.17. Otras provisiones

Ninguna estipulación.