Política de Certificación

Información general

Control documental

Clasificación de seguridad:	Público
Versión:	1
Fecha edición:	06/11/2024
Fichero:	ENVIOGT_PC_v1.r4

Estado formal

Preparado por:	Revisado por:	Aprobado por:
Nombre: Laura Paniagua Fecha: 06/11/2024	Nombre: Fecha:	Nombre: Fecha:

Control de versiones

Versión	Partes que cambian	Descripción del cambio	Autor del cambio	Fecha del cambio
1	Original	Creación del documento	LPO	06/11/2024

Índice

1. Introducción

1.1. Presentación

Este documento constituye las políticas de Certificación de ENVIOGT S.A., (en lo sucesivo ENVIOGT) en relación con la prestación de sus servicios de certificación digital de acuerdo con la normativa legalmente aplicable.

Los certificados que se emiten son los siguientes:

- De Persona Natural Ciudadano
- De Persona Natural Vinculado a empresa u organización.
- De Persona Natural Colegiado o associado.
- De Persona Natural Empleado Público.
- De Persona Natural Representante.
- De Persona Jurídica.
- De Estampado Cronológico (Sello de Tiempo).

1.2. Nombre del documento e identificación

Este documento es la "Política de Certificación de ENVIOGT.

1.3. Descripción de la política

La ENVIOGT ha asignado a cada política de certificado un identificador de objeto (OID), para su identificación por las aplicaciones.

Número OID	Tipo de certificados
	Persona Natural
1.3.6.1.4.1. 62432.1.1.1	*De Persona Natural Ciudadano*
1.3.6.1.4.1. 62432.1.1.1	*Certificado de Persona Natural vinculado a Empresa u Organización*
1.3.6.1.4.1. 62432.1.1.1	*Certificado de Persona Natural Colegiado*
1.3.6.1.4.1. 62432.1.1.1	*Certificado de Persona Natural Empleado Público*
	Persona Natural Representante
1.3.6.1.4.1. 62432.1.2.1	*Certificado Representante Legal*

	Persona jurídica
1.3.6.1.4.1. 62432.1.3.1	*Certificado de Persona Jurídica*
	Estampado cronológico
1.3.6.1.4.1. 62432.1.9.1	*Certificado de sello de tiempo*

1.4. Participantes en los servicios de certificación

1.4.1. Prestador de servicios de certificación

El prestador de servicios de certificación es la persona jurídica, que expide y gestiona certificados para entidades finales, empleando una Autoridad de Certificación, o presta otros servicios relacionados con la firma electrónica.

ENVIOGT es un prestador de servicios de certificación que actúa de conformidad con las previsiones del Decreto No. 47-2008 de Ley para el Reconocimiento de las Comunicaciones y Firmas Electrónicas, su reglamento, así como las normas técnicas que establece el Registro de Prestadores de Servicios de Certificación aplicables a la expedición y gestión de certificados de firma electrónica avanzada, al objeto de facilitar el cumplimiento de los requisitos legales y el reconocimiento internacional de sus servicios.

1.4.2. Autoridad de Registro

La Autoridad de Registro es ENVIOGT y en consecuencia es la entidad encargada de:

- Tramitar las solicitudes de certificados.
- Identificar al solicitante y comprobar que cumple con los requisitos necesarios para la solicitud de los certificados.
- Validar las circunstancias personales de la persona que constará como firmante/suscriptor del certificado.
- Gestionar la generación de claves y la emisión del certificado, o hacer entrega del certificado al suscriptor o de los medios para su generación.
- Custodiar la documentación relativa a la identificación y registro de los firmantes y/o suscriptores y gestión del ciclo de vida de los certificados.

1.4.3. Entidades finales

Las entidades finales son las personas u organizaciones destinatarias de los servicios de emisión, gestión y uso de certificados digitales, para los usos de autenticación y firma electrónica.
Serán entidades finales de los servicios de certificación de ENVIOGT las siguientes:

1. Suscriptores del servicio de certificación
2. Firmantes
3. Partes usuarias

1.4.3.1. Suscriptores del servicio de certificación

Los suscriptores del servicio de certificación son:

- Las empresas, entidades, corporaciones u organizaciones que los adquieren a ENVIOGT (directamente o a través de un tercero) para su uso en su ámbito corporativo empresarial, corporativo u organizativo, y se encuentran identificados en los certificados.
- Las personas naturales que adquieren los certificados para sí mismas, y se encuentran identificados en los certificados.

1.4.3.2. Firmantes

Los firmantes son las personas naturales que poseen de forma exclusiva las claves de firma electrónica para autenticación y/o firma electrónica avanzada; pudiendo ser personas típicamente empleados, representantes legales o voluntarios, así como otras personas vinculadas a los suscriptores; incluyendo las personas al servicio de las Administraciones Públicas, en los certificados de empleado público.

Los firmantes se encuentran debidamente autorizados por el suscriptor y debidamente identificados en el certificado mediante su nombre y apellidos, y número de identificación inequívoco, sin que sea posible, en general, el empleo de seudónimos.

La clave privada de un firmante no puede ser recuperada o deducida por el prestador de servicios de certificación, por lo que las personas naturales identificadas en los correspondientes certificados son las únicas responsables de su protección y deben considerar las implicaciones de perder una clave privada.

Dada la existencia de certificados para usos diferentes de la firma electrónica, como la autenticación, también se emplea el término más genérico de “persona natural

identificada en el certificado", siempre con pleno respeto al cumplimiento de la regulación de firma electrónica en relación con los derechos y obligaciones del firmante.

1.4.3.3. Partes usuarias

Las partes usuarias son las personas y las organizaciones que reciben firmas electrónicas y certificados digitales.

Como paso previo a confiar en los certificados, las partes usuarias deben verificarlos, como se establece en la Declaración de Prácticas de Certificación y en las correspondientes instrucciones disponibles en la página web del ENVIOGT como Prestador de Servicios de Certificación.

1.4.4. Proveedor de Servicios de Infraestructura de Clave Pública

ENVIOGT y UANATACA, S.A.U han suscrito un contrato de prestación de servicios de tecnología en el que UANATACA proveerá la infraestructura de clave pública (PKI) que sustenta el servicio de certificación de ENVIOGT. Así mismo UANATACA pone a disposición de ENVIOGT el personal técnico necesario para correcto desempeño de las funciones fiables propias de un Prestador de Servicios de Certificación.

Dicho lo cual, UANATACA se configura como el proveedor de servicios de Infraestructura para servicios de certificación, provee sus servicios tecnológicos a ENVIOGT para que éste pueda llevar a cabo los servicios inherentes a un Prestador de Servicios de Certificación, garantizando en todo momento la continuidad de los servicios en las condiciones y bajo los requisitos exigidos por la normativa.

Asimismo, se informa que UANATACA es un Prestador de Servicios de Confianza acreditado conforme las previsiones del Reglamento Europeo No. 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE (Reglamento eIDAS).

La PKI de UANATACA se somete a auditorías anuales para la evaluación de la conformidad de prestadores cualificados de servicios de confianza de acuerdo con la normativa aplicable, bajo las normas:

a) ISO/IEC 17065:2012
b) ETSI EN 319 403
c) ETSI EN 319 421
d) ETSI EN 319 401
e) ETSI EN 319 411-2
f) ETSI EN 319 411-1

Asimismo la PKI de UANATACA se somete a auditorías anuales bajo los estándares de seguridad:

a) ISO 9001:2015
b) ISO/IEC 27001:2014

1.5. Uso y limitaciones

Esta sección lista las aplicaciones para las que puede emplearse cada tipo de certificado, establece limitaciones a ciertas aplicaciones y prohíbe ciertas aplicaciones de los certificados.

1.5.1. Periodo de validez de los certificados

El periodo de validez será el que se indique en el propio certificado, con un máximo de 3 años.

1.5.2. Usos permitidos para los certificados

Se deben tener en cuenta los usos permitidos indicados en los diversos campos de los perfiles de certificados, disponibles en el web: https://enviogt.com/legal/dpc/

1.5.2.1. Certificado de Persona Natural Ciudadano

Este certificado dispone del OID 1.3.6.1.4.1.62432.1.1.1 Es un certificado que se emite para la autenticación y la firma electrónica avanzada, de acuerdo con las disposiciones del Decreto No. 47-2008 de Ley para el Reconocimiento de las Comunicaciones y Firmas Electrónicas.

Este certificado se emite para personas individuales nacionales o extranjeras y garantiza la identidad del firmante del servicio electrónico de certificación, y permite la generación de la "firma electrónica avanzada", es decir, la firma electrónica que está vinculada al firmante de manera única, permitiendo su identificación y ha sido generada utilizando medios que el firmante puede mantener bajo su control exclusivo, vinculada a los datos a que se refiere, de modo tal que cualquier cambio ulterior de los mismos es detectable.

La firma electrónica avanzada generada a través de este certificado tendrá, respecto de los datos consignados en forma electrónica, el mismo valor jurídico que la firma manuscrita en relación con los consignados en papel y será admisible como prueba en juicio conforme a las previsiones del artículo 33 de la Ley para el Reconocimiento de las Comunicaciones y Firmas Electrónicas.

Los certificados se pueden utilizar en aplicaciones como las que se indican a continuación:

a) Autenticación en sistemas de control de acceso.
b) Firma de correo electrónico seguro.
c) Otras aplicaciones de firma electrónica, de acuerdo con lo que acuerden las partes o con las normas jurídicas aplicables en cada caso.

El campo "key usage" tiene activadas y por tanto permite realizar, las siguientes funciones:

a) Firma digital (Digital Signature, para realizar la función de autenticación).
b) Compromiso con el contenido (Content commitment, para realizar la función de firma electrónica avanzada).
c) Key Encipherment.

1.5.2.2. Certificado de Persona Natural vinculado a Empresa u Organización

Este certificado dispone del OID 1.3.6.1.4.1.62432.1.1.1 Es un certificado que se emite para la autenticación y la firma electrónica avanzada, de acuerdo con las disposiciones del Decreto No. 47-2008 de Ley para el Reconocimiento de las Comunicaciones y Firmas Electrónicas.

Este Certificado se emite para personas nacionales o extranjeras y garantiza la identidad del suscriptor y del firmante, y una relación entre el firmante y una entidad, empresa u organización descrita en el campo "O" (Organization), y permite la generación de la "firma electrónica avanzada", es decir, la firma electrónica que está

vinculada al firmante de manera única, permitiendo su identificación y ha sido generada utilizando medios que el firmante puede mantener bajo su control exclusivo, vinculada a los datos a que se refiere, de modo tal que cualquier cambio ulterior de los mismos es detectable.

La firma electrónica avanzada generada a través de este certificado tendrá, respecto de los datos consignados en forma electrónica, el mismo valor jurídico que la firma manuscrita en relación con los consignados en papel y será admisible como prueba en juicio conforme a las previsiones del artículo 33 de la Ley para el Reconocimiento de las Comunicaciones y Firmas Electrónicas.

Los certificados se pueden utilizar en aplicaciones como las que se indican a continuación:

a) Autenticación en sistemas de control de acceso.
b) Firma de correo electrónico seguro.
c) Otras aplicaciones de firma electrónica, de acuerdo con lo que acuerden las partes o con las normas jurídicas aplicables en cada caso.

El campo “key usage” tiene activadas y por tanto permite realizar, las siguientes funciones:

a) Firma digital (Digital Signature, para realizar la función de autenticación).
b) Compromiso con el contenido (Content commitment, para realizar la función de firma electrónica avanzada).
c) Key Encipherment.

1.5.2.3. Certificado de Persona Natural Colegiado

Este certificado dispone del OID 1.3.6.1.4.1.62432.1.1.1 Es un certificado que se emite para la autenticación y la firma electrónica avanzada, de acuerdo con las disposiciones del Decreto No. 47-2008 de Ley para el Reconocimiento de las Comunicaciones y Firmas Electrónicas.

Este certificado se emite a personas individuales nacionales o extranjeras y garantiza la identidad del firmante del servicio electrónico de certificación y su registro o inscripción ante una entidad o colegio habilitante para el ejercicio profesional descrito en el campo “O” (Organization), permitiendo la generación de la “firma electrónica avanzada”, es decir, la firma electrónica que está vinculada al firmante de manera única, permitiendo su identificación y ha sido generada utilizando medios que el firmante puede mantener

bajo su control exclusivo, vinculada a los datos a que se refiere, de modo tal que cualquier cambio ulterior de los mismos es detectable.

La firma electrónica avanzada generada a través de este certificado tendrá, respecto de los datos consignados en forma electrónica, el mismo valor jurídico que la firma manuscrita en relación con los consignados en papel y será admisible como prueba en juicio conforme a las previsiones del artículo 33 de la Ley para el Reconocimiento de las Comunicaciones y Firmas Electrónicas.

Los certificados se pueden utilizar en aplicaciones como las que se indican a continuación:

a) Autenticación en sistemas de control de acceso.
b) Firma de correo electrónico seguro.
c) Otras aplicaciones de firma electrónica, de acuerdo con lo que acuerden las partes o con las normas jurídicas aplicables en cada caso.

El campo “key usage” tiene activadas y por tanto permite realizar, las siguientes funciones:

a) Firma digital (Digital Signature, para realizar la función de autenticación).
b) Compromiso con el contenido (Content commitment, para realizar la función de firma electrónica avanzada).
c) Key Encipherment.

1.5.2.4. Certificado de Persona Natural Empleado Público

Este certificado dispone del OID 1.3.6.1.4.1.62432.1.1.1 Es un certificado que se emite para la autenticación y la firma electrónica avanzada, de acuerdo con las disposiciones del Decreto No. 47-2008 de Ley para el Reconocimiento de las Comunicaciones y Firmas Electrónicas.

Este certificado se emite a personas individuales nacionales o extranjeras y garantiza la identidad del suscriptor y del firmante, y una relación entre el firmante y una Institución pública descrita en el campo “O” (Organization), y permite la generación de la “firma electrónica avanzada”, es decir, la firma electrónica que está vinculada al firmante de manera única, permitiendo su identificación y ha sido generada utilizando medios que el firmante puede mantener bajo su control exclusivo, vinculada a los datos a que se refiere, de modo tal que cualquier cambio ulterior de los mismos es detectable.

La firma electrónica avanzada generada a través de este certificado tendrá, respecto de los datos consignados en forma electrónica, el mismo valor jurídico que la firma manuscrita en relación con los consignados en papel y será admisible como prueba en juicio conforme a las previsiones del artículo 33 de la Ley para el Reconocimiento de las Comunicaciones y Firmas Electrónicas.

Los certificados se pueden utilizar en aplicaciones como las que se indican a continuación:

a) Autenticación en sistemas de control de acceso.
b) Firma de correo electrónico seguro.
c) Otras aplicaciones de firma electrónica, de acuerdo con lo que acuerden las partes o con las normas jurídicas aplicables en cada caso.

El campo “key usage” tiene activadas y por tanto permite realizar, las siguientes funciones:

a) Firma digital (Digital Signature, para realizar la función de autenticación).
b) Compromiso con el contenido (Content commitment, para realizar la función de firma electrónica avanzada).
c) Key Encipherment.

1.5.2.5. Certificado de Representante Legal

Este certificado dispone del OID 1.3.6.1.4.1.62432.1.2.1 Es un certificado que se emite para la autenticación y la firma electrónica avanzada, de acuerdo con las disposiciones del Decreto No. 47-2008 de Ley para el Reconocimiento de las Comunicaciones y Firmas Electrónicas.

Este certificado se emite a personas individuales nacionales o extranjeras y el uso de este certificado garantiza la identidad del suscriptor y del firmante, y una relación de representación legal o apoderamiento entre el firmante y la entidad, empresa u organización descrita en el campo “O” (Organization), y permite la generación de la “firma electrónica avanzada”, es decir, la firma electrónica que está vinculada al firmante de manera única, permitiendo su identificación y ha sido generada utilizando medios que el firmante puede mantener bajo su control exclusivo, vinculada a los datos a que se refiere, de modo tal que cualquier cambio ulterior de los mismos es detectable.

La firma electrónica avanzada generada a través de este certificado tendrá, respecto de los datos consignados en forma electrónica, el mismo valor jurídico que la firma manuscrita en relación con los consignados en papel y será admisible como prueba en

juicio conforme a las previsiones del artículo 33 de la Ley para el Reconocimiento de las Comunicaciones y Firmas Electrónicas.

Los certificados se pueden utilizar en aplicaciones como las que se indican a continuación:

a) Autenticación en sistemas de control de acceso.
b) Firma de correo electrónico seguro.
c) Otras aplicaciones de firma electrónica, de acuerdo con lo que acuerden las partes o con las normas jurídicas aplicables en cada caso.

El campo "key usage" tiene activadas y por tanto permite realizar, las siguientes funciones:

a) Firma digital (Digital Signature, para realizar la función de autenticación).
b) Compromiso con el contenido (Content commitment, para realizar la función de firma electrónica avanzada).
c) Key Encipherment.

1.5.2.6. Certificado de persona jurídica

Este certificado dispone del OID 1.3.6.1.4.1.62432.1.3.1 Es un certificado que se emite para la autenticación y la firma electrónica avanzada de una persona jurídica, de acuerdo con las disposiciones del Decreto No. 47-2008 de Ley para el Reconocimiento de las Comunicaciones y Firmas Electrónicas.

Estos certificados identifican a una persona jurídica de derecho público o privado, entidad del Estado o persona jurídica comerciante y garantizan la identidad de la empresa, entidad u organización suscriptora identificada en el certificado, y en su caso la del responsable de gestionar el certificado (si se hubiese identificado). Este certificado permite la generación de la "firma electrónica avanzada", es decir, la firma electrónica que está vinculada al firmante (entidad, empresa u organización) de manera única, permitiendo su identificación y ha sido generada utilizando medios que puede mantener bajo su control exclusivo, vinculada a los datos a que se refiere, de modo tal que cualquier cambio ulterior de los mismos es detectable.

La firma electrónica avanzada generada a través de este certificado tendrá, respecto de los datos consignados en forma electrónica, el mismo valor jurídico que la firma manuscrita en relación con los consignados en papel y será admisible como prueba en juicio conforme a las previsiones del artículo 33 de la Ley para el Reconocimiento de las Comunicaciones y Firmas Electrónicas.

Los certificados se pueden utilizar en aplicaciones como las que se indican a continuación:

a) Autenticación en sistemas de control de acceso.
b) Firma de correo electrónico seguro.
c) Otras aplicaciones de firma electrónica, de acuerdo con lo que acuerden las partes o con las normas jurídicas aplicables en cada caso.

El campo "key usage" tiene activadas y por tanto permite realizar, las siguientes funciones:

a) Firma digital (Digital Signature, para realizar la función de autenticación).
b) Compromiso con el contenido (Content commitment, para realizar la función de firma electrónica avanzada).
c) Key Encipherment.

1.5.2.7. Certificado de estampado cronológico

Este certificado dispone del OID 1.3.6.1.4.1.62432.1.9.1 Los certificados de sellos de tiempo o de estampado cronológico, son certificados emitidos para la operación de autoridades de sellado de tiempo, para la firma de sellos de tiempo que estas producen.

Estos certificados permiten la firma de los sellos de tiempo, que se emiten desde el momento que hayan obtenido un certificado de sello de tiempo válido y mientras este se encuentre vigente.

1.5.3. Límites y prohibiciones de uso de los certificados

Los certificados se emplean para su función propia y finalidad establecida, sin que puedan emplearse en otras funciones y con otras finalidades.

Del mismo modo, los certificados deben emplearse únicamente de acuerdo con la regulación aplicable, especialmente teniendo en cuenta las restricciones de importación y exportación existentes en cada momento.

Los certificados no pueden emplearse para firmar certificados de clave pública de ningún tipo, ni firmar listas de revocación de certificados (LRC).

Los certificados no se han diseñado, no se pueden destinar y no se autoriza su uso o reventa como 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.

Se deben tener en cuenta los límites indicados en los diversos campos de los perfiles de certificados, disponibles en el documento de políticas de certificación publicado en la web de ENVIOGT en https://firma-e.com.gt.

El empleo de los certificados digitales en operaciones que contravienen esta Declaración de Prácticas de Certificación, los documentos jurídicos vinculantes con cada certificado, o los contratos con las autoridades de registro o con sus firmantes/suscriptores, tiene la consideración de uso indebido a los efectos legales oportunos, eximiéndose por tanto a ENVIOGT, en función de la legislación vigente, de cualquier responsabilidad por este uso indebido de los certificados que realice el firmante o cualquier tercero.

ENVIOGT no tiene acceso a los datos sobre los que se puede aplicar el uso de un certificado. Por lo tanto, y como consecuencia de esta imposibilidad técnica de acceder al contenido del mensaje, no es posible por parte de ENVIOGT emitir valoración alguna sobre dicho contenido, asumiendo por tanto el suscriptor, el firmante o la persona responsable de la custodia, cualquier responsabilidad que provenga del contenido aparejado al uso de un certificado.

Asimismo, le será imputable al suscriptor, al firmante o a la persona responsable de la custodia, cualquier responsabilidad que pudiese derivarse de la utilización del mismo fuera de los límites y condiciones de uso recogidas en esta Declaración de Prácticas de Certificación, los documentos jurídicos vinculantes con cada certificado, o los contratos o convenios con las autoridades de registro o con sus suscriptores, así como de cualquier otro uso indebido del mismo derivado de este apartado o que pueda ser interpretado como tal en función de la legislación vigente.

1.5.4. Certificados de corta duración

Los certificados de corta duración son certificados expedidos con una duración limitada, cuya validez máxima es de veinticuatro (24) horas y cuyo uso está limitado exclusivamente a una transacción de firma para la cual se emitió. Inmediatamente después de su uso, la clave privada se deshabilita imposibilitando su uso posterior hasta su caducidad. Una transacción puede contener varios documentos dentro de una única solicitud de transacción para la que se genera el certificado electrónico.

2. Identificación y autenticación

2.1. Registro inicial

2.1.1. Tipos de nombres

Todos los certificados contienen un nombre distintivo (DN o *distinguished name*) conforme al estándar X.509 en el campo *Subject*, incluyendo un componente *Common Name* (CN=), relativo a la identidad del suscriptor y de la persona natural identificada en el certificado, así como diversas informaciones de identidad adicionales en el campo *SubjectAlternativeName*.

Los nombres contenidos en los certificados son los siguientes:

2.1.1.1. Certificado de Persona individual

Country Name	País de residencia o nacionalidad del firmante
Surname	Apellidos del firmante (como consta en el documento oficial)
Given Name	Nombre del firmante (como consta en el documento oficial)
Serial Number	Número del Documento Personal de Identificación (DPI) o Pasaporte del firmante codificado acorde a ETSI EN 319 412-1. Ejemplo: (“IDCGT-1234567890123")
Tax Identification Number	Número de Identificación Tributario (NIT) del firmante codificado acorde a ETSI EN 319 412-1. Ejemplo: ("TINGT-15770650")
Common Name	NOMBRE Y APELLIDOS DEL FIRMANTE
Street	Dirección de residencia del firmante
Locality	Localidad de residencia del firmante

2.1.1.2. Certificado de Relación con entidad

Country Name	País de residencia o nacionalidad del firmante
Organization Name	Se especificará el nombre de la organización a la que pertenece el firmante
Organizational Unit Name	Se especificará el Departamento al que pertenece el firmante o el tipo de vinculación con la organización
Organization Identifier	Número de identificación Tributario (NIT) de la persona jurídica a la que está vinculado el firmante, en formato ETSI EN 319412-1. (Ejemplo: “VATGT-44081080).
Title	Se especificará el nombre del título o puesto que la persona ocupa en la organización.
Surname	Apellidos del firmante (como consta en el documento oficial)
Given Name	Nombre del firmante (como consta en el documento oficial)
Serial Number	Número del Documento Personal de Identificación (DPI) o Pasaporte del firmante codificado acorde a ETSI EN 319 412-1 Example: (“IDCGT-1234567890123")

Tax Identification Number	Número de identificación Tributario (NIT) del firmante codificado acorde a ETSI EN 319 412-1. Example: ("TINGT-15770650")
Common Name	Se especificará: "Given name" + "Surname" + " / " + "Organization name" Example "GABRIEL GARCIA MARTINEZ / UANATACA"
Street	Dirección de residencia del firmante
Locality	Localidad de residencia del firmante

2.1.1.3. Certificado de Profesional titulado

Country Name	País de residencia o nacionalidad del firmante.
Organization Name	Se especificará el nombre del Colegio Oficial, de la asociación o del registro de profesionales
Organizational Unit Name	Se especificará en general "Colegiado", "Asociado", "Registrado Profesional" más el número de profesional. Ejemplo: Colegiado nº4631316
Title	Se especificará el título, especialidad o profesión del firmante
Surname	Apellidos del firmante (como consta en el documento oficial)
Given Name	Nombre del firmante (como consta en el documento oficial)
Serial Number	Número del Documento Personal de Identificación (DPI) o Pasaporte del firmante codificado acorde a ETSI EN 319 412-1. Example: ("IDCGT-1234567890123")
Tax Identification Number	Número de identificación Tributario (NIT) del firmante codificado acorde a ETSI EN 319 412-1. Example: ("TINGT-15770650")
Common Name	Se especificará el nombre y apellidos de la persona, espacio, /, espacio / title, espacio / y número de profesional que le fue asignado. Example "GABRIEL GARCIA MARTINEZ / Abogado y Notario / Colegiado:09250"
Street	Dirección de residencia del firmante
Locality	Localidad de residencia del firmante

2.1.1.4. Certificado de Funcionario público

Country Name	País de residencia o nacionalidad del firmante
Organization Name	Se especificará el nombre de la entidad pública a la que está vinculado
Organizational Unit Name	Se especificará por defecto "FUNCIONARIO PUBLICO"
Organization Identifier	Número de identificación Tributario (NIT) de la persona jurídica a la que está vinculado el firmante, en formato ETSI EN 319412-1. (Ejemplo: "VATGT-44081080).
Title	Se especificará el título, especialidad o cargo del firmante.
Surname	Apellidos del firmante (como consta en el documento oficial)
Given Name	Nombre del firmante (como consta en el documento oficial)
Serial Number	Número del Documento Personal de Identificación (DPI) o Pasaporte del firmante codificado acorde a ETSI EN 319 412-1.

	Example: (“IDCGT-1234567890123")
Tax Identification Number	Código Único de Identificación oficial del firmante codificado acorde a ETSI EN 319 412-1. Example: ("TINGT-15770650")
Common Name	Se especificará: "Given name" + "Surname" + " / " + "Organization name" . Example "GABRIEL GARCIA MARTINEZ / UANATACA"
Street	Dirección de residencia del firmante
Locality	Localidad de residencia del firmante

2.1.1.5. Certificado de Representante Legal

Country Name	País de residencia o nacionalidad del firmante
Organization Name	Organización de la que el firmante es representante
Organizational Unit Name	Se especificará el Departamento al que pertenece representante
Organization Identifier	Número de identificación Tributario (NIT) de la persona jurídica representada, en formato ETSI EN 319412-1. (Ejemplo: “VATGT-44081080).
Title	Representante legal
Surname	Apellidos del representante (como consta en el documento oficial)
Given Name	Nombre del representante (como consta en el documento oficial)
Serial Number	Número del Documento Personal de Identificación (DPI) o Pasaporte del representante codificado acorde a ETSI EN 319 412-1. Example: (“IDCGT-1234567890123")
Tax Identification Number	Código Único de Identificación oficial del representante codificado acorde a ETSI EN 319 412-1. Example: ("TINGT-15770650")
Common Name	Se especificará: "Given name" + "Surname" + " / " + "Organization name" ". Example "GABRIEL GARCIA MARTINEZ / UANATACA"
Street	Dirección de residencia del firmante
Locality	Localidad de residencia del firmante

2.1.1.6. Certificado de persona jurídica

Country Name	País de residencia o nacionalidad de la Persona Jurídica
Organization Name	Nombre de la Empresa, Organización o Entidad
Organizational Unit Name	Nombre del departamento que utilizará el certificado
Organization Identifier	Número de identificación Tributario (NIT) de la persona jurídica, en formato ETSI EN 319412-1. (Ejemplo: “VATGT-44081080).
Serial Number	Número de identificación Tributario (NIT) de la persona jurídica SIN el prefijo VATGT. (Ejemplo: “44081080).
Common Name	Nombre de la Empresa, Organización o Entidad. Example “UANATACA "

Street	Dirección de residencia de la persona jurídica
Locality	Localidad de residencia de la persona jurídica

2.1.1.7. Certificado de estampado cronológico

Country Name	País de residencia o nacionalidad de la Persona Jurídica
Organization Name	Nombre de la Empresa, Organización o Entidad
Organizational Unit Name	Nombre del departamento que utilizará el certificado
Organization Identifier	Número de identificación Tributario (NIT) de la persona jurídica, en formato ETSI EN 319412-1. (Ejemplo: "VATGT-44081080).
Common Name	Nombre de la Empresa, Organización o Entidad incluyendo una identificación de única para cada certificado (Ejemplo: Cámara Comercio TSU01)
Street	Dirección de residencia de la persona jurídica
Locality	Localidad de residencia de la persona jurídica

2.1.2. Significado de los nombres

Los nombres contenidos en los campos *SubjectName* y *SubjectAlternativeName* de los certificados son comprensibles en lenguaje natural, de acuerdo con lo establecido en la sección anterior.

2.1.3. Emisión de certificados de pruebas

En el caso que los datos indicados en el DN o Subject fueran ficticios (ej. "Test Organization", "Test Nombre", "Apellido1") o se indique expresamente palabras que denoten su invalidez (ej. "TEST", "PRUEBA" o "INVALIDO"), se considerará al certificado sin validez legal y por lo tanto sin responsabilidad alguna sobre ENVIOGT. Estos certificados se emiten para realizar pruebas técnicas de interoperabilidad y permitir al ente regulador su evaluación.

2.1.4. Empleo de anónimos y seudónimos

En ningún caso se pueden utilizar seudónimos para identificar una entidad, empresa u organización, ni a un firmante. Así mismo, en ningún caso se emiten certificados anónimos.

2.1.5. Interpretación de formatos de nombres

Los formatos de nombres se interpretarán de acuerdo con la ley del país de establecimiento del suscriptor, en sus propios términos.

El campo “país” o “estado” será el del suscriptor del certificado.

Los certificados cuyos suscriptores sean personas jurídicas, entidades u organismos de la administración pública, muestran la relación entre estas y una persona natural, con independencia de la nacionalidad de la persona natural.

En el campo “número de serie” se incluye el DPI, Pasaporte u otro número de identificación idóneo del firmante, reconocido en derecho.

2.2. Validación inicial de la identidad

La identidad de los suscriptores de certificados resulta fijada en el momento de la firma del contrato entre ENVIOGT y el suscriptor, momento en el que se verifica la existencia del suscriptor mediante su documento oficial de identidad y los requisitos establecidos según el perfil de cada certificado, al igual que los poderes de actuación de la persona que presente como representante si fuese el caso. Para esta verificación, se podrá emplear documentación pública o notarial, o la consulta directa a los registros públicos correspondientes.

En el caso de personas naturales identificadas en certificados cuyo suscriptor sea una persona jurídica, sus identidades se validarán mediante la presentación de su documento oficial de identificación o mediante los registros corporativos de la entidad, empresa u organización de derecho público o privado, suscriptoras de los certificados. En este último caso, el suscriptor producirá una certificación de los datos necesarios, y la remitirá a ENVIOGT, por los medios que ésta habilite, para el registro de la identidad de los firmantes.

Los ficheros de datos personales de cada entidad, empresa u organización de derecho público o privado a que se refiere el párrafo anterior son responsabilidad de cada organización, siendo su responsabilidad, y no la de ENVIOGT.

La validación de identidad del suscriptor se podrá realizar de forma presencial o de manera virtual a través de los mecanismos implementados por ENVIOGT, en cumplimiento a las guías establecidas por el Registro de Prestadores de Servicios de Certificación RPSC del Ministerio de Economía de la República de Guatemala.

2.2.1. Autenticación de la identidad de una organización, empresa o entidad mediante representante

Las personas naturales con capacidad de actuar en nombre de las personas jurídicas u organizaciones suscriptoras en general, podrán actuar como representantes de las mismas, siempre y cuando exista una situación previa de representación legal o voluntaria entre la persona natural y la organización de la que se trate, que exige su reconocimiento por ENVIOGT, sus autoridades de registro y/o terceros vinculados, la cual se realizará mediante el siguiente procedimiento:

1. El representante del suscriptor se identificará ante un operador o persona autorizada de una Autoridad de Registro de ENVIOGT, acreditando el carácter y facultades que alegue poseer. Alternativamente, a los mismos efectos ENVIOGT podrá poner a disposición de los suscriptores un formulario para su cumplimiento previo.

2. El representante proporcionará la siguiente información y sus correspondientes soportes acreditativos:
    - Sus datos de identificación, como representante:
        - Nombre y apellidos
        - Lugar y fecha de nacimiento
        - Documento de identidad idóneo reconocido en derecho para la identificación del representante
    - Los datos de identificación del suscriptor al que representa:
        - Denominación o razón social.
        - Información de registro existente, que puede incluir los datos relativos a la constitución, personalidad jurídica, extensión y vigencia de las facultades de representación del solicitante.
        - Documento: documento acreditativo de la identificación fiscal de la organización suscriptora.
        - Documentos que sirvan para acreditar los extremos citados de manera fehaciente y su inscripción en el correspondiente registro público si así resulta exigible. La citada comprobación podrá realizarse, asimismo, mediante consulta en el registro público en el que estén inscritos los documentos de constitución y de apoderamiento, pudiendo emplear los medios telemáticos facilitados por los citados registros públicos.
    - Los datos relativos a la representación o la capacidad de actuación que ostenta:

- La vigencia de la representación o la capacidad de actuación (fecha de inicio y fin) si resulta aplicable.
- El ámbito y los límites, en su caso, de la representación o de la capacidad de actuación:
    - TOTAL. Representación o capacidad total. Esta comprobación se podrá realizar mediante consulta telemática al registro público donde conste inscrita la representación.
    - PARCIAL. Representación o capacidad parcial. Esta comprobación se podrá realizar mediante copia auténtica o electrónica de la escritura notarial de apoderamiento, en los términos de la normativa notarial.

3. El operador o personal autorizado de la Autoridad de Registro de ENVIOGT comprobará la identidad del representante mediante la presentación de su documento de identidad y se podrá realizar de forma presencial o de manera virtual a través de los mecanismos implementados por ENVIOGT u otro medio idóneo reconocido en derecho para su identificación, así como el contenido de la representación con la documentación.

4. El operador o personal autorizado de la Autoridad de Registro de ENVIOGT verificará la información suministrada para la autenticación y le devolverá la documentación original aportada.

5. Alternativamente, se podrá legitimar notarialmente la firma del formulario, y hacerse llegar al operador o personal autorizado de la Autoridad de Registro ENVIOGT, en cuyo caso los pasos 3 y 4 anteriores no serán precisos.

La prestación del servicio de certificación se formaliza mediante el oportuno contrato entre ENVIOGT y el suscriptor, debidamente representado.

2.2.2. Autenticación de la identidad de una persona natural

Esta sección describe los métodos de comprobación de la identidad de una persona natural identificada en un certificado.

2.2.2.1. En los certificados

La identidad de las personas naturales firmantes identificados en los certificados, se valida mediante la presentación de su documento oficial de identificación (Documento Nacional de Identidad, tarjeta de identidad, pasaporte u otro medio idóneo reconocido en derecho para su identificación).

La información de identificación de las personas naturales identificadas en los certificados cuyo suscriptor sea una entidad pública o privada, con o sin personalidad jurídica, la información podrá ser validada comparando la información de la solicitud con los registros de la entidad, empresa u organización de derecho público o privado a la que está vinculado, o bien con la documentación que esta haya suministrado sobre la persona natural que identifica como firmante, asegurando la corrección de la información a certificar.

2.2.2.2. Validación de la Identidad

Para la solicitud de certificados, el operador o personal autorizado de la Autoridad de Registro ENVIOGT valida la identidad del solicitante, para lo cual la persona natural deberá exhibir documento de identidad (DPI, Pasaporte u otro medio idóneo reconocido en derecho para su identificación).

Para la solicitud de los certificados cuyo suscriptor sea una persona jurídica los mismos pueden ser tramitados cuando medie un documento idóneo para la verificación de los extremos establecidos en esta Política de Certificación y la Declaración de Prácticas de Certificación. Sin embargo, la entrega del certificado o de las respectivas credenciales de generación y acceso deben deberán realizarse a persona autorizada del suscriptor, con la correspondiente verificación de su identidad.

2.2.2.3. Vinculación de la persona natural

La justificación documental de la vinculación de una persona natural identificada en un certificado con la entidad, empresa u organización de derecho público o privado viene dada por su constancia en los registros internos (contrato de trabajo como empleado, o el contrato mercantil que lo vincula, o el acta donde se indique su cargo, o la solicitud como miembro de la organización…) de cada una de las personas públicas y privadas a las que están vinculadas.

2.3. Identificación y autenticación de solicitudes de renovación

2.3.1. Validación para la renovación rutinaria de certificados

Antes de renovar un certificado, el operador o personal autorizado de la Autoridad de Registro comprueba que la información empleada para verificar la identidad y los restantes datos del suscriptor y de la persona natural identificada en el certificado continúan siendo válidos.

Los métodos aceptables para dicha comprobación son:

- Los métodos aceptables para dicha comprobación son alguno de los Verificación presencial de la solicitud de la renovación del certificado.
- Solicitud de renovación del certificado digital realizada firmada con firma electrónica avanzada basada en certificado vigente para el momento de su renovación, siempre que no haya cambios en la información contenida en el mismo.

Si cualquier información del suscriptor o de la persona natural identificada en el certificado ha cambiado, se registra adecuadamente la nueva información y se produce una identificación completa, de acuerdo con lo establecido en la sección 2.2.

2.3.2. Identificación y autenticación de la solicitud de renovación

Antes de renovar un certificado, el operador o personal autorizado de la Autoridad de Registro comprobará que la información empleada en su día para verificar la identidad y los restantes datos del suscriptor y de la persona natural identificada en el certificado continúa siendo válida, en cuyo caso se aplicará lo dispuesto en la sección anterior.

La renovación de certificados tras la revocación no será posible en los siguientes casos:

- El certificado fue revocado por emisión errónea a una persona diferente a la identificada en el certificado.
- El certificado fue revocado por emisión no autorizada por la persona natural identificada en el certificado.
- El certificado revocado puede contener información errónea o falsa.

Si cualquier información del suscriptor o de la persona natural identificada en el certificado ha cambiado, se registra adecuadamente la nueva información y se produce una identificación completa, de acuerdo con lo establecido en la sección 2.2.

2.4. Identificación y autenticación de la solicitud de revocación, suspensión o reactivación

ENVIOGT o un operador o personal autorizado de la Autoridad de Registro autentica las peticiones e informes relativos a la revocación, suspensión o reactivación de un certificado, comprobando que provienen de una persona autorizada.

La identificación de los suscriptores y/o firmantes en el proceso de revocación, suspensión o reactivación de certificados podrá ser realizada por:

- El suscriptor y/o firmante:
    - Identificándose y autenticándose mediante el uso del Código de Revocación (ERC o ERC) a través de la página web de ENVIOGT en horario 24 horas al día 7 días a la semana.
    - Otros medios de comunicación, como el teléfono, correo electrónico, etc. cuando existan garantías razonables de la identidad del solicitante de la suspensión o revocación, a juicio de ENVIOGT y/o Autoridades de Registro.
- Las autoridades de registro deberán identificar al firmante ante una petición de revocación, suspensión o reactivación según los propios medios que considere necesarios.

Cuando en horario de oficina el suscriptor desee iniciar una petición de revocación y existan dudas para su identificación, su certificado pasa a estado de suspensión.

3. Requisitos de operación del ciclo de vida de los certificados

3.1. Solicitud de emisión de certificado

3.1.1. Legitimación para solicitar la emisión

La emisión de un certificado puede ser solicitada por el suscriptor o el firmante en cada caso, cumpliendo los requisitos previstos en esta Política de Certificación y la Declaración de Prácticas de Certificación de ENVIOGT.

3.1.2. Procedimiento de alta y responsabilidades

ENVIOGT gestiona las altas de las solicitudes de certificados basado en la información proporcionada por el suscriptor al momento de la solicitud. El suscriptor es responsable de la veracidad de esta documentación en los términos en esta Política de Certificación y la Declaración de Prácticas de Certificación de ENVIOGT.

3.2. Procesamiento de la solicitud de certificación

3.2.1. Ejecución de las funciones de identificación y autenticación

ENVIOGT se asegura antes de emitir un certificado que la solicitud cumpla con los requisitos previstos en esta Política de Certificación y la Declaración de Prácticas de Certificación de ENVIOGT. Las evidencias recogidas en el proceso son resguardadas por ENVIOGT por el tiempo legal correspondiente.

3.2.2. Aprobación o rechazo de la solicitud

En caso de que los datos se verifiquen correctamente, ENVIOGT aprueba la solicitud del certificado y proceder a su emisión y entrega.

3.3. Emisión del certificado

Tras la aprobación de la solicitud de certificación se procede a la emisión del certificado de forma segura y se pone a disposición del firmante para su aceptación.

Los procedimientos establecidos en esta sección también se aplican en caso de renovación de certificados, dado que la misma implica la emisión de un nuevo certificado.

Durante el proceso, ENVIOGT:

- Protege la confidencialidad e integridad de los datos de registro de que dispone.
- Utiliza 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.
- Genera el par de claves, mediante un procedimiento de generación de certificados vinculado de forma segura con el procedimiento de generación de claves.
- Emplea un procedimiento de generación de certificados que vincula de forma segura el certificado con la información de registro, incluyendo la clave pública certificada.
- Se asegura de que el certificado es emitido por sistemas que utilicen protección contra falsificación y que garanticen la confidencialidad de las claves durante el proceso de generación de dichas claves.
- Indica la fecha y la hora en que se expidió un certificado.
- Garantiza el control exclusivo de las claves por parte del usuario, no pudiendo la propia ENVIOGT o sus Autoridades de Registro deducirlas o utilizarlas en ningún modo.

3.4. Entrega y aceptación del certificado

La aceptación del certificado por la persona natural identificada en el certificado se produce mediante la firma de la hoja de entrega y aceptación.

3.5. Uso del par de claves y del certificado

3.5.1. Uso por el firmante

Los firmantes se obligan a:

- Facilitar a ENVIOGT información completa y adecuada, conforme a los requisitos de esta Política de Certificación y la Declaración de Prácticas de Certificación, en especial en lo relativo al procedimiento de registro.
- Manifestar su consentimiento previo a la emisión y entrega de un certificado.
- Emplear el certificado de acuerdo con lo establecido en las políticas y prácticas de certificación de ENVIOGT.
- Reconocer la capacidad de producción de firmas electrónicas avanzadas mediante el certificado emitido por ENVIOGT; esto es, equivalentes a firmas manuscritas, así como otros tipos de firmas electrónicas y mecanismos de cifrado de información.
- Ser especialmente diligente en la custodia de su clave privada y/o las credenciales de acceso a la misma, con el fin de evitar usos no autorizados, de acuerdo con lo establecido en la Declaración de Prácticas de Certificación.
- Comunicar a ENVIOGT, Autoridades de Registro y a cualquier persona que se crea que pueda confiar en el certificado, sin retrasos injustificables:
    - La pérdida, el robo o el compromiso potencial de su clave privada.
    - La pérdida de control sobre su clave privada, debido al compromiso de los datos de activación (por ejemplo, el código PIN) o por cualquier otra causa.
    - Las inexactitudes o cambios en el contenido del certificado que conozca o pudiera conocer el suscriptor.
- Dejar de emplear la clave privada transcurrido correspondiente.

El firmante queda obligado a responsabilizarse de:

- Que todas las informaciones suministradas por el firmante que se encuentran contenidas en el certificado son correctas.
- Que el certificado se emplea exclusivamente para usos legales y autorizados, de acuerdo con la Declaración de Prácticas de Certificación.
- Que ninguna persona no autorizada ha tenido jamás acceso a la clave privada del certificado, y que es el único responsable de los daños causados por su incumplimiento del deber de proteger la clave privada.
- Que el firmante es una entidad final y no un prestador de servicios de certificación, y que no empleará la clave privada correspondiente a la clave

pública listada en el certificado para firmar certificado alguno (o cualquier otro formato de clave pública certificada), ni Lista de Revocación de Certificados, ni título de prestador de servicios de certificación ni en ningún otro caso.

3.5.2. Uso por el subscriptor

3.5.2.1. Obligaciones del suscriptor del certificado

El suscriptor queda obligado contractualmente a:

- Facilitar al Prestador de Servicios de Certificación información completa y adecuada, conforme a los requisitos de esta Política de Certificación y la Declaración de Prácticas de Certificación, en especial en lo relativo al procedimiento de registro.
- Manifestar su consentimiento previo a la emisión y entrega de un certificado.
- Emplear el certificado de acuerdo con lo establecido en las políticas y prácticas de certificación de ENVIOGT en su condición de Prestador de Servicios de Certificación.
- Comunicar a ENVIOGT, Autoridades de Registro y a cualquier persona que el suscriptor crea que pueda confiar en el certificado, sin retrasos injustificables:
    - La pérdida, el robo o el compromiso potencial de su clave privada.
    - La pérdida de control sobre su clave privada, debido al compromiso de los datos de activación (por ejemplo, el código PIN) o por cualquier otra causa.
    - Las inexactitudes o cambios en el contenido del certificado que conozca o pudiera conocer el suscriptor.
    - La pérdida, la alteración, el uso no autorizado, el robo o el compromiso, cuando exista, de la tarjeta.
- Trasladar a las personas naturales identificadas en el certificado el cumplimiento de las obligaciones específicas de los mismos, y establecer mecanismos para garantizar el efectivo cumplimiento de estas.
- No monitorizar, manipular o realizar actos de ingeniería reversa sobre la implantación técnica de los servicios de certificación sin permiso previo por escrito.
- No comprometer la seguridad de los servicios de certificación del prestador de servicios de certificación.

3.5.2.2. Responsabilidad civil del suscriptor de certificado

ENVIOGT obliga contractualmente al suscriptor a responsabilizarse de:

- Que todas las manifestaciones realizadas en la solicitud son correctas.
- Que todas las informaciones suministradas por el suscriptor que se encuentran contenidas en el certificado son correctas.
- Que el certificado se emplea exclusivamente para usos legales y autorizados, de acuerdo con la Declaración de Prácticas de Certificación.
- Que ninguna persona no autorizada ha tenido jamás acceso a la clave privada del certificado, y que es el único responsable de los daños causados por su incumplimiento del deber de proteger la clave privada.
- Que el suscriptor es una entidad final y no un prestador de servicios de certificación, y que no empleará la clave privada correspondiente a la clave pública listada en el certificado para firmar certificado alguno (o cualquier otro formato de clave pública certificada), ni Lista de Revocación de Certificados, ni título de prestador de servicios de certificación ni en ningún otro caso.

3.5.3. Uso por el tercero que confía en certificados

3.5.3.1. Obligaciones del tercero que confía en certificados

Se informa al tercero que confía en certificados de que el mismo debe asumir las siguientes obligaciones:

- Asesorarse de forma independiente acerca del hecho de que el certificado es apropiado para el uso que se pretende.
- Verificar la validez, suspensión o revocación de los certificados emitidos, para lo que empleará información sobre el estado de los certificados.
- Verificar todos los certificados de la jerarquía de certificados, antes de confiar en la firma digital o en alguno de los certificados de la jerarquía
- Reconocer que las firmas electrónicas verificadas basadas en certificados emitidos por ENVIOGT como Prestador de Servicios de Certificación debidamente autorizado para operar como tal por el Registro de Prestadores de Servicios de Certificación, tienen la consideración legal de firmas electrónicas avanzadas; esto es, equivalentes a firmas manuscritas.
- Tener presente cualquier limitación en el uso del certificado, con independencia de que se encuentre en el propio certificado o en el contrato de tercero que confía en el certificado.

- Tener presente cualquier precaución establecida en un contrato o en otro instrumento, con independencia de su naturaleza jurídica.
- No monitorizar, manipular o realizar actos de ingeniería reversa sobre la implantación técnica de los servicios de certificación sin permiso previo por escrito.
- No comprometer la seguridad de los servicios de certificación.

3.5.3.2. Responsabilidad civil del tercero que confía en certificados

ENVIOGT informa al tercero que confía en certificados de que el mismo debe asumir las siguientes responsabilidades:

- Que dispone de suficiente información para tomar una decisión informada con el objeto de confiar en el certificado o no.
- Que es el único responsable de confiar o no en la información contenida en el certificado.
- Que será el único responsable si incumple sus obligaciones como tercero que confía en el certificado.

3.6. Renovación de certificados

La renovación de los certificados exige la renovación de claves, de acuerdo con lo establecido en la Declaración de Prácticas de Certificación de ENVIOGT.

3.7. Revocación, suspensión o reactivación de certificados

La revocación de un certificado supone la pérdida de validez definitiva del mismo, y es irreversible.

La suspensión (o revocación temporal) de un certificado supone la pérdida de validez temporal del mismo, y es reversible. Sólo los certificados de entidad final podrán ser suspendidos.

La reactivación de un certificado supone su paso de estado suspendido a estado activo.

3.7.1. Procedimientos de solicitud de revocación, suspensión o reactivación

La entidad que precise revocación, suspensión o reactivación un certificado puede solicitarlo directamente a ENVIOGT o a la Autoridad de Registro del suscriptor o realizarlo él mismo a través del servicio online disponible en la página web de ENVIOGT. Los certificados emitidos bajo la modalidad One-Shot únicamente se podrá tramitar la revocación solicitándolo directamente a ENVIOGT o a la Autoridad de Registro del suscriptor.

La solicitud de revocación, suspensión o reactivación deberá incorporar la siguiente información:

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

La solicitud debe ser autenticada, antes de proceder a la revocación, suspensión o reactivación.

El servicio de revocación, suspensión o reactivación se encuentra en la página web de ENVIOGT en la dirección: https://enviogt.com

En caso de que el destinatario de una solicitud de revocación, suspensión o reactivación por parte de una persona natural identificada en el certificado fuera la entidad suscriptora, una vez autenticada la solicitud debe remitir una solicitud en este sentido a ENVIOGT.

La solicitud de revocación, suspensión o reactivación será procesada a su recepción, y se informará al suscriptor y, en su caso, a la persona natural identificada en el certificado, acerca del cambio de estado del certificado.

Tanto el servicio de gestión de revocación, suspensión o reactivación como el servicio de consulta son considerados servicios críticos y así constan en el Plan de contingencias y el plan de continuidad de negocio de ENVIOGT.

3.7.2. Obligación de consulta de información de revocación o suspensión de certificados

Los terceros deben comprobar el estado de aquellos certificados en los cuales desean confiar.

Un método por el cual se puede verificar el estado de los certificados es consultando la Lista de Revocación de Certificados más reciente emitida por el Prestador de Servicios de Certificación ENVIOGT.

Las Listas de Revocación de Certificados se publican en el Depósito de la Autoridad de Certificación, así como en las siguientes direcciones web, indicadas dentro de los certificados:

- http://crl1.uanataca.com/public/pki/crl/CA2subordinada.crl
- http://crl2.uanataca.com/public/pki/crl/CA2subordinada.crl

El estado de la vigencia de los certificados también se puede comprobar por medio del protocolo OCSP.

- http://ocsp1.uanataca.com/public/pki/ocsp/
- http://ocsp2.uanataca.com/public/pki/ocsp/

3.7.3. Obligación de consulta de servicios de comprobación de estado de certificados

Resulta obligatorio consultar el estado de los certificados antes de confiar en los mismos.

4. Perfiles de certificados y listas de certificados revocados

4.1. Perfil de certificado

Todos los certificados emitidos bajo esta Política de Certificación cumplen con el estándar X.509 versión 3 y el RFC 3739 y los diferentes perfiles descritos en la norma EN 319 412.

4.1.1. Número de versión

ENVIOGT emite certificados X.509 Versión 3.

4.1.2. Identificadores de objeto (OID) de los algoritmos

El identificador de objeto del algoritmo de firma es:

- 1.2.840.113549.1.1.11 sha256WithRSAEncryption

El identificador de objeto del algoritmo de la clave pública es:

- 1.2.840.113549.1.1.1 rsaEncryption

4.2. Perfil de la lista de revocación de certificados

4.2.1. Número de versión

Las CRL emitidas por ENVIOGT son de la versión 2.

4.2.2. Perfil de OCSP

Según el estándar IETF RFC 6960.

5. Anexo I – Acrónimos y glosario

AC	Autoridad de Certificación
CA	Certification Authority. Autoridad de Certificación
RA	Autoridad de Registro
CP	Certificate Policy
CPS	Certification Practice Statement. Declaración de Prácticas de Certificación
CRL	Certificate Revocation List. Lista de certificados revocados
CSR	Certificate Signing Request. Petición de firma de certificado
DES	Data Encryption Standard. Estándar de cifrado de datos
DN	Distinguished Name. Nombre distintivo dentro del certificado digital
DSA	Digital Signature Algorithm. Estándar de algoritmo de firma
DSCF	Dispositivo Seguro de Creación de Firma
SSCD	Secure Signature Creation Device. Dispositivo Seguro de Creación de Firma
FIPS	Federal Information Processing Standard Publication
ISO	International Organization for Standardization. Organismo Internacional de Estandarización
LDAP	Lightweight Directory Access Protocol. Protocolo de acceso a directorios
OCSP	On-line Certificate Status Protocol. Protocolo de acceso al estado de los certificados
OID	Object Identifier. Identificador de objeto
PA	Policy Authority. Autoridad de Políticas
PC	Política de Certificación
PIN	Personal Identification Number. Número de identificación personal
PKI	Public Key Infrastructure. Infraestructura de clave pública
RSA	Rivest-Shimar-Adleman. Tipo de algoritmo de cifrado
SHA	Secure Hash Algorithm. Algoritmo seguro de Hash
SSL	Secure Sockets Layer
TCP/IP	Transmission Control. Protocol/Internet Protocol
NTP	Network Time Protocol. Protocolo. Protocolo de internet para sincronizar relojes de sistemas informáticos.
Blob	Binary Large Objects. Objetos Binarios Grandes