BIT4ID SAC

POLÍTICA DE CERTIFICACIÓN

Información general

Control documental

Clasificación de seguridad:	Público
Entidad de destino:	BIT4ID SAC
Versión:	2.1
Fecha edición:	29/06/2020
Fichero:	BIT4IDSAC_PC_v2.1

Estado formal

Preparado por:	Revisado por:	Aprobado por:
Nombre: Alejandro Grande Fecha: 29/06/2020	Nombre: Albert Borrás Fecha: 29/06/2020	Nombre: Jorge García Fecha: 29/06/2020

Control de versiones

Versión	Partes que cambian	Descripción del cambio	Autor del cambio	Fecha del cambio
1.0	Original	Creación del documento	ABD	16/11/2017
2.0	Completo	Ajuste de la terminología aplicada en la versión original del documento, así como modificación del formato de este, para adaptar a las necesidades del ente regulador.	AGB	11/05/2020
2.1	1.6	Se modifican apartados de los perfiles, eliminando el Key Encipherment.	AGB	29/06/2020

Índice

1. Introducción

1.1. Presentación

Bit4id, S.A.C., en lo sucesivo "Bit4id" es una sociedad mercantil registrada en Perú especializada en el desarrollo de sistemas para la gestión de la identidad digital y la firma electrónica, y que presta servicios de certificación, especialmente aquellos relacionados con la gestión del ciclo de vida de certificados digitales, mediante la explotación de la infraestructura de llave pública (PKI) de Uanataca, S.A., empresa registrada de acuerdo a la legislación española, que tiene por objeto la Prestación de Servicios de Confianza Cualificados conforme a 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 a la normativa aplicable, bajo las normas ISO/IEC 17065:2012, ETSI EN 319 403 V2.2.2., ETSI EN 319 421 v1.1.1, ETSI EN 319 401 v2.1.1, ETSI EN 319 411-2 v 2.1.1, ETSI EN 319 411-1 v 1.1.1., ETSI EN 319 401 v2.1.1, ETSI EN 319 411-2 v 2.1.1 ETSI EN 319 411-1 v 1.1.1, ETSI EN 319 401 v2.1.1.

1.2. Objetivo

Este documento declara la Política de certificación de Bit4id, los cuales dan cumplimiento a los requisitos establecidos por la Ley de Firmas y Certificados Digitales (Ley 27269), su reglamento con la regulación emitida por el Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (INDECOPI) en su condición de (Autoridad Administrativa Competente o AAC).

Los certificados que se emiten son los siguientes:

- **De PERSONAS**
  - Certificado de Persona Natural - Ciudadano
- **De Persona Jurídica**
  - Certificado de Perteneciente a una organización
  - Certificado para Facturación Electrónica
  - Certificado de Agente automatizado
  - Certificado de Sello de Tiempo

1.3. Nombre del documento e identificación

Este documento es la "Política de Certificación de Bit4id".

1.3.1. Identificadores de certificados

Bit4id ha asignado a cada política de certificado un identificador de objeto (OID), para su identificación por las aplicaciones.

Número OID	Políticas de certificados
1.3.6.1.4.1.47286.2.2.1.1	*Ciudadano*
1.3.6.1.4.1.47286.2.2.2.1	*Perteneciente a Organización*
1.3.6.1.4.1.47286.2.2.2.2	*Facturación Electrónica*
1.3.6.1.4.1.47286.2.2.2.3	*Agente automatizado*
1.3.6.1.4.1.47286.2.2.5	*Sello de tiempo*

1.4. Participantes en los servicios de certificación

Acreditación: acto a través del cual la Autoridad Administrativa Competente, previo cumplimiento de las exigencias establecidas en la Ley, en su Reglamento y en las disposiciones dictadas por ella, faculta a las entidades solicitantes reguladas en el Reglamento a prestar los

servicios solicitados en el marco de la Infraestructura Oficial de Firma Electrónica.

Agente automatizado: procesos y equipos programados para atender requerimientos predefinidos y dar una respuesta automática sin intervención humana, en dicha fase.

Autenticación: proceso técnico que permite determinar la identidad de la persona que firma electrónicamente, en función del mensaje firmado por éste y al cual se le vincula. Este proceso no otorga certificación notarial ni fe pública.

Autoridad Administrativa Competente (AAC): organismo público responsable de acreditar a las entidades de certificación y a las entidades de registro o verificación, de reconocer los estándares tecnológicos aplicables en la Infraestructura Oficial de Firma Electrónica, de supervisar dicha Infraestructura y las otras funciones señaladas en el Reglamento o aquellas que requiera en el transcurso de sus operaciones. Dicha responsabilidad recae en el Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual – INDECOPI.

Certificado digital: documento electrónico generado y firmado digitalmente por una entidad de certificación el cual vincula un par de claves con una persona natural o jurídica confirmando su identidad.

Clave privada: es una de las claves de un sistema de criptografía asimétrica que se emplea para generar una firma digital sobre un mensaje de datos y es mantenida en reserva por el titular de la firma digital.

Clave pública: es la otra clave en un sistema de criptografía asimétrica que es usada por el destinatario de un mensaje de datos para verificar la firma digital puesta en dicho mensaje. La clave pública puede ser conocida por cualquier persona.

Código de verificación (hash o resumen): secuencia de bits de longitud fija obtenida como resultado de procesar un mensaje de datos con un algoritmo, de tal manera que: (1) El mensaje de datos produzca siempre el mismo código de verificación cada vez que se le aplique dicho algoritmo. (2) Sea improbable, a través de medios técnicos, que el mensaje de datos pueda ser derivado o reconstruido a partir del código de verificación producido por el algoritmo. (3) Sea improbable que, por medios técnicos, se pueda encontrar dos mensajes de datos que produzcan el mismo código de verificación al usar el mismo algoritmo.

Declaración de prácticas de certificación (CPS): documento oficialmente presentado por una entidad de certificación a la Autoridad Administrativa Competente, mediante el cual define sus Prácticas de Certificación.

Declaración de prácticas de registro o verificación (RPS): documento oficialmente presentado por una entidad de Registro o Verificación a la Autoridad Administrativa Competente, mediante el cual define sus Prácticas de Registro o Verificación.

Entidad de certificación (EC): persona jurídica pública o privada que presta indistintamente servicios de producción, emisión, gestión, cancelación u otros servicios inherentes a la certificación digital. Asimismo, puede asumir las funciones de registro o verificación.

Entidad de Registro o Verificación (ER): persona jurídica, con excepción de los notarios públicos, encargada del levantamiento de datos, comprobación de éstos respecto a un solicitante de un mecanismo de firma electrónica o certificación digital, la aceptación y autorización de las solicitudes para la emisión de un mecanismo de firma electrónica o certificados digitales, así como de la aceptación y autorización de las solicitudes de cancelación de mecanismos de firma electrónica o certificados digitales. Las personas encargadas de ejercer la citada función serán supervisadas y reguladas por la normatividad vigente.

Estándares técnicos internacionales: requisitos de orden técnico y de uso internacional que deben observarse en la emisión de firmas electrónicas y en las prácticas de certificación.

Infraestructura Oficial de Firma Electrónica (IOFE): sistema confiable, acreditado, regulado y supervisado por la Autoridad Administrativa Competente, provisto de instrumentos legales y técnicos que permiten generar firmas electrónicas y proporcionar diversos niveles de seguridad respecto a: 1) la integridad de los mensajes de datos y documentos electrónicos; 2) la identidad de su autor, lo que es regulado conforme a la Ley. El sistema incluye la generación de firmas electrónicas, en la que participan entidades de certificación y entidades de registro o verificación acreditadas ante la Autoridad Administrativa Competente, incluyendo a la Entidad de Certificación Nacional para el Estado Peruano (ECERNEP), las Entidades de Certificación para el Estado Peruano
(ECEP) y las Entidades de Registro o Verificación para el Estado Peruano (EREP).

Medios telemáticos: conjunto de bienes y elementos técnicos informáticos que en unión con las telecomunicaciones permiten la generación, procesamiento, transmisión, comunicación y archivo de datos e información.

Políticas de Certificación (CP): documento oficialmente presentado por una entidad de certificación a la Autoridad Administrativa Competente, mediante el cual establece, entre otras cosas, los tipos de certificados digitales que podrán ser emitidos, cómo se deben emitir y gestionar los certificados, y los respectivos derechos y responsabilidades de las Entidades de Certificación. Para el caso de una EC Raíz, la CP incluye las directrices para la gestión del Sistema de Certificación de las ECs vinculadas.

Suscriptor o titular de la firma digital: persona natural responsable de la generación y uso de la clave privada, a quien se le vincula de manera

exclusiva con un mensaje de datos firmado digitalmente utilizando su clave privada. En el caso que el titular del certificado sea una persona natural, sobre la misma recaerá la responsabilidad de suscriptor.

1.5. Participantes en los servicios de certificación

1.5.1. Entidad de certificación

La Entidad de Certificación es la persona, natural o jurídica, que expide y gestiona certificados para entidades finales o presta otros servicios relacionados con la certificación digital. Bit4id presta el servicio de certificación digital basado en la infraestructura tecnológica de UANATACA, S.A., identificada al inicio de este documento.

Para la prestación de los servicios de certificación, Bit4id ha establecido una jerarquía de entidades de certificación utilizando la infraestructura tecnológica a cargo del Prestador de Servicios de Confianza español UANATACA, S.A. de la siguiente forma:

1.5.1.1. UANATACA ROOT 2016

Se trata de la entidad de certificación raíz de la jerarquía que emite certificados a otras entidades de certificación, y cuyo certificado de clave público ha sido auto firmado.

Datos de identificación:

CN:	UANATACA ROOT 2016
Huella digital:	6d c0 84 50 a9 5c d3 26 62 c0 91 0f 8c 2d ce 23 0d 74 66 ad
Válido desde:	Viernes, 11 de marzo de 2016
Válido hasta:	Lunes, 11 de marzo de 2041
Longitud de clave RSA:	4.096 bits

1.5.1.2. UANATACA CA1 2016

Se trata de la entidad de certificación dentro de la jerarquía que emite los certificados a las entidades finales, y cuyo certificado de clave pública ha sido firmado digitalmente por la UANATACA ROOT 2016.

Datos de identificación:

CN:	UANATACA CA2 2016
Huella digital:	0e ce 52 78 03 c9 db 6e 63 bc ea 55 36 b9 3a e8 28 4e 8d 2d
Válido desde:	Viernes, 11 de marzo de 2016
Válido hasta:	Domingo, 11 de marzo de 2029
Longitud de clave RSA:	4.096 bits

1.5.1.3. UANATACA CA2 2016

Se trata de la entidad de certificación dentro de la jerarquía que emite los certificados a las entidades finales, y cuyo certificado de clave pública ha sido firmado digitalmente por la UANATACA ROOT 2016.

Datos de identificación:	
CN:	UANATACA CA1 2016
Huella digital:	7f 2c b4 f7 69 22 4c b0 cf 8b 69 27 51 cb d4 cc 64 a2 c4 50
Válido desde:	Viernes, 11 de marzo de 2016
Válido hasta:	Domingo, 11 de marzo de 2029
Longitud de clave RSA:	4.096 bits

1.5.2. Autoridad de Registro

Una Autoridad de Registro (RA) 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 del certificado.
- Gestionar la generación de claves y la emisión del certificado.
- 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.

Podrán actuar como Autoridad de Registro de Bit4id, cualquier Entidad de Registro debidamente acreditada y registrada ante la Autoridad Administrativa Competente y que cuente con la correspondiente autorización y acuerdo con Bit4id.

Bit4idformalizará contractualmente las relaciones entre ella misma y cada una de las entidades que actúen como Autoridad de Registro de Bit4id. Asimismo, publicará en la página web https://web.uanataca.com/pe los convenios y la documentación legal necesaria de cada Autoridad de Registro con la que se encuentra vinculada.

La entidad que actúe como Autoridad de Registro de Bit4id podrá autorizar a una o varias personas como Operador de la RA para operar con el sistema de emisión de certificados de Bit4id.

Las Autoridades de Registro podrán delegar las funciones de identificación de los suscriptores y/o firmantes, previo acuerdo de colaboración en el que se acepte la delegación de estas funciones, previa autorización de Bit4id.
También podrán ser Autoridades de Registro sujetas a este documento, las unidades designadas para esta función por los suscriptores de los certificados, como un departamento de personal, dado que disponen de los registros auténticos acerca de la vinculación de los firmantes con el suscriptor.

1.5.3. Proveedor de Servicios de Infraestructura de Servicios de Certificación

UANATACA, S.A. se configura como el proveedor de servicios de Infraestructura para servicios de certificación, provee sus servicios tecnológicos a Bit4id S.A.C. para que este pueda llevar a cabo los servicios inherentes a una Entidad de Certificación, garantizando en todo momento la continuidad de los servicios en las condiciones y bajo los requisitos exigidos por la normativa.

1.5.4. 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 BIT4ID las siguientes:

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

1.5.4.1. Suscriptores del servicio de certificación

Los suscriptores del servicio de certificación son:

- Las empresas, entidades, corporaciones u organizaciones que adquieren certificados de Bit4id 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.

El suscriptor del servicio de certificación adquiere una licencia de uso del certificado, para su uso propio, o al objeto de facilitar la certificación de la identidad de una persona concreta debidamente autorizada para diversas actuaciones en el ámbito organizativo del suscriptor – certificados de firma digital. En este último caso, esta persona figura identificada en el certificado.

El suscriptor del servicio de certificación es, por tanto, el cliente del prestador de servicios de certificación, de acuerdo con la legislación privada, y tiene los derechos y obligaciones que se definen por la Entidad de Certificación, que son adicionales y se entienden sin perjuicio de los derechos y obligaciones de los firmantes, como se autoriza y regula en las normas técnicas aplicables a la expedición de certificados digitales.

1.5.4.2. Firmantes

Los firmantes son las personas naturales que poseen de forma exclusiva las claves de firma digital para autenticación y/o firma electrónica; siendo típicamente los empleados, agentes, representantes legales, así como otras personas vinculadas a los suscriptores, en el caso de que los haya.

Los firmantes se encuentran debidamente autorizados por el suscriptor y debidamente identificados en el certificado mediante su nombre y apellidos, y número de identificación unívoco que permite su

identificación inequívoca, sin que sea posible, en general, el empleo de seudónimos.

La clave privada de un firmante no puede ser recuperada o deducida por Bit4id, por lo que las personas naturales identificadas en los correspondientes certificados son las únicas responsables de su protección y deberían considerar las implicaciones de perder una clave privada.

Dada la existencia de certificados para usos diferentes de la firma digital, 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 digital en relación con los derechos y obligaciones del firmante.

1.5.4.3. Partes usuarias

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

Como paso previo a confiar en los certificados, las partes usuarias deben verificarlos, como se establece en esta declaración de prácticas de certificación y en las correspondientes instrucciones disponibles en https://web.uanataca.com/pe

1.5.4.4. Tercero que confía

El tercero que confía incluye a todas aquellas personas naturales y/o jurídicas que deciden aceptar y confiar en los certificados digitales emitidos por Bit4id como Entidad de Certificación.
El Tercero que confía puede ser suscriptor o no de un certificado.

1.6. Uso de los certificados

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.

1.6.1. 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://web.uanataca.com/pe.

1.6.1.1. Certificados de PERSONAS

1.6.1.1.1. Certificado de Persona Natural - Ciudadano

Este certificado dispone del OID 1.3.6.1.4.1.47286.2.2.1.1. Es un certificado emitido en el marco de la Infraestructura Oficial de Firma Electrónica acuerdo a la Ley de Firmas y Certificados Digitales y su Reglamento, para la autenticación y firma digital de personas naturales.

Estos certificados garantizan la identidad de la persona indicada en el certificado, y permiten la generación de la firma digital en los términos previstos en el artículo 6 del Reglamento de la Ley de Firmas y Certificados Digitales.

También se puede utilizar en aplicaciones que no requieren la firma digital equivalente a la firma manuscrita, como las aplicaciones 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.

La información de usos en el perfil de certificado indica lo siguiente:
El campo "key usage" tiene activadas y por tanto nos 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)

1.6.1.2. Certificados de Persona Jurídica

1.6.1.2.1. Certificado de Perteneciente a una organización

Este certificado dispone del OID 1.3.6.1.4.1.47286.2.2.2.1. Es un certificado emitido dentro de la Infraestructura Oficial de Firma Electrónica de acuerdo a la Ley de Firmas y Certificados Digitales y su Reglamento, para la autenticación y firma digital de personas naturales que pertenezcan a una entidad u organización.

Estos certificados garantizan la identidad de la persona indicada en el certificado, y permiten la generación de la firma digital en los términos previstos en el artículo 6 del Reglamento de la Ley de Firmas y Certificados Digitales.

También se puede utilizar en aplicaciones que no requieren la firma digital equivalente a la firma manuscrita, como las aplicaciones 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.

La información de usos en el perfil de certificado indica lo siguiente:

El campo "key usage" tiene activadas y por tanto nos permite realizar, la siguiente función:

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)

1.6.1.2.2. Certificado para Facturación Electrónica

Este certificado dispone del OID 1.3.6.1.4.1.47286.2.2.2.2. Es un certificado emitido dentro de la Infraestructura Oficial de Firma Electrónica de acuerdo a la Ley de Firmas y Certificados Digitales y su Reglamento, para la autenticación y firma digital que acreditan vinculación con una persona jurídica.

Estos certificados garantizan la identidad de la persona indicada en el certificado, y permiten la generación de la firma digital en los términos previstos en el artículo 6 del Reglamento de la Ley de Firmas y Certificados Digitales.

La información de usos en el perfil de certificado indica lo siguiente:
El campo "key usage" tiene activadas y por tanto nos 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)

Este certificado solo podrá ser utilizado para la Facturación Electrónica de la empresa identificada en el certificado y por tanto cualquier otra operación no autorizada tendrá la consideración de usos indebidos de conformidad con la normativa aplicable.

1.6.1.2.3. Certificado de Agente Automatizado

Este certificado dispone del OID 1.3.6.1.4.1.47286.2.2.2.3. Es un certificado que se emite dentro de la Infraestructura Oficial de Firma Electrónica de acuerdo a la Ley de Firmas y Certificados Digitales y su Reglamento, para la identificación y firma de entidades u organizaciones.

Estos certificados garantizan la identidad de la entidad u organización suscriptora vinculada que se identifica en el certificado, y en su caso la del responsable de gestionar el mismo. La información de usos en el perfil de certificado indica lo siguiente:

a) El campo "key usage" tiene activadas, y por tanto nos 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)

1.6.1.3. Certificado de Sello de Tiempo

Este certificado dispone del OID 1.3.6.1.4.1.47286.2.2.5. Es un certificado que se emite dentro de la Infraestructura Oficial de Firma Electrónica de acuerdo a la Ley de Firmas y Certificados Digitales y su Reglamento, para la firma de evidencias digitales de tiempo electrónico para la identificación y firma de entidades u organizaciones.

La información de usos en el perfil de certificado indica lo siguiente:

a) El campo "key usage" tiene activadas, y por tanto permite realizar, las siguientes funciones:
    a. Compromiso con el contenido (Content commitment, para realizar la función de firma digital)
b) En el campo "extKeyUsage" se dispone de forma activada de la indicación:
    a. "timeStamping" para realizar la función de sellado de tiempo electrónico.

El campo "User Notice" describe el uso de este certificado

1.6.2. 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, ni 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 la web.

El empleo de los certificados digitales en operaciones que contravienen esta documento, los documentos jurídicos vinculantes con cada certificado, o los contratos con las entidades de registro o con sus firmantes/suscriptores, tiene la consideración de uso indebido a los efectos legales oportunos, eximiéndose por tanto a Bit4id como Entidad de Certificación, en función de la legislación vigente, de cualquier

responsabilidad por este uso indebido de los certificados que realice el firmante o cualquier tercero.

Bit4id 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 Bit4id emitir valoración alguna sobre dicho contenido, asumiendo por tanto el suscriptor, el firmante o la persona responsable de la custodia, cualquier responsabilidad dimanante 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 este Documento, los documentos jurídicos vinculantes con cada certificado, o los contratos o convenios con las entidades 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.

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.501 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. Certificados de PERSONAS

2.1.1.1.1. Certificado de Persona Natural - Ciudadano

Country (C)	Estado[1]
Surname	Apellidos del firmante
Given Name	Nombre(s) del firmante
Serial Number	DNI/Carné de Extranjería/Pasaporte/ u otro número de identificación idóneo del firmante, reconocido en derecho
Common Name (CN)	Nombre y apellidos del firmante

[1] El campo "Estado" corresponderá al del país de la nacionalidad o residencia del firmante.

2.1.1.2. Certificados de Persona Jurídica

2.1.1.2.1. Certificado de Perteneciente a una organización

Country (C)	Estado[2]
Organization (O)	Empresa, Entidad, Organización, Colegio u asociación profesional a la que está vinculado el firmante
Organization Unit (OU)	Unidad de la Organización a la que está vinculado el firmante, si se tratase de un profesional colegiado se especificará "Colegiado".
Organization Identifier	RUC de la Organización a la que está vinculado el firmante
Title	Título o especialidad de firmante
Surname	Apellidos del firmante
Given Name	Nombre(s) del firmante
Serial Number	DNI/Carné de Extranjería/Pasaporte/ u otro número de identificación idóneo del firmante, reconocido en derecho
Common Name (CN)	Nombre y apellidos del firmante

[2] El campo "Estado" corresponderá al del estado donde se produzca la relación contractual entre el firmante y la entidad a la que está vinculado (por ser empleado, miembro, socio u otra vinculación), con independencia de la nacionalidad del trabajador.

2.1.1.2.2. Certificado de Facturación Electrónica

Country	País donde la entidad está registrada
Common Name	Nombres y Apellidos del firmante
Given Name	Nombre del firmante (como consta en el documento oficial)
Surname	Apellidos del firmante (como consta en el documento oficial)
Title	Cargo del firmante (Ej. GERENTE GENERAL)
Organizational Unit	RUC de la Organización (Ej. "20555049464")
Organizational Unit	Denominación o nombre del departamento
Organization Name	Nombre de la empresa a la que se le emite el certificado digital
Kind of personal ID document	Tipo de documento de identificación
Company ID document	Número identificativo de la empresa
Kind of company ID document	Tipo de identificativo de la empresa
Serial Number	Número de documento oficial de la persona física solicitante
State or Province (S)	Estado o Provincia
Locality Name	Ciudad
Description	"Certificado para Facturación Electrónica"

2.1.1.3. Certificado de Agente Automatizado

Country (C)	Estado donde está registrada la Organización
Organization (O)	Nombre de la Organización
Organization Unit (OU)	Denominación de la unidad emisora
Organization Identifier	RUC o Número de identificación fiscal de la Organización a la que está vinculado el sello electrónico
Surname	Apellidos del responsable del certificado
Given Name	Nombre(s) del responsable del certificado
Serial Number	RUC o Número de identificación fiscal de la Organización a la que está vinculado el sello electrónico
Common Name (CN)	Nombre del sistema automátizado

2.1.1.4. Certificado de Sello de Tiempo

Country (C)	Estado donde está registrada la Organización
Organization (O)	Nombre de la Organización
Organization Unit (OU)	Denominación de la unidad emisora
Organization Identifier	RUC o Número de identificación fiscal de la Organización que responsable del servicio de sellado de tiempo
Locality Name (L)	Localidad donde está registrada la Organización
Common Name (CN)	Sello de tiempo de la organizaicón

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.

2.1.2.1. Emisión de certificados del set de pruebas y certificados de pruebas en general

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 Bit4id. Estos certificados se emiten para realizar pruebas técnicas de interoperabilidad y/o permitir al ente regulador su evaluación.

2.1.3. Empleo de anónimos y seudónimos

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

2.1.4. 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 DNI, Carné de Extranjería, Pasaporte u otro número de identificación idóneo del firmante, reconocido en derecho.

2.1.5. Unicidad de los nombres

Los nombres de los suscriptores de certificados serán únicos, para cada política de certificado.

No se podrá asignar un nombre de suscriptor que ya haya sido empleado, a un suscriptor diferente, situación que, en principio no se ha de dar, gracias a la presencia del número del Número de Identificación Fiscal, o equivalente, en el esquema de nombres.

Un suscriptor puede pedir más de un certificado siempre que la combinación de los siguientes valores existentes en la solicitud fuera diferente de un certificado válido:

- DNI, Carné de Extranjería/Pasaporte/Registro Único de Contribuyentes (RUC) u otro identificador legalmente válido de la persona natural.
- Registro Único de Contribuyentes (RUC) u otro identificador legalmente válido del suscriptor.
- Tipo de certificado (OID de identificador de política de certificación).
- Soporte del certificado.

Como excepción, esta DPC permite emitir un certificado cuando coincida RUC del suscriptor, DNI/Carné de Extranjería del firmante, Tipo de certificado, Soporte del certificado, con un certificado activo, siempre que exista algún elemento diferenciador entre ambos, en los campos cargo (title) y/o departamento (Organizational Unit).

2.1.6. Resolución de conflictos relativos a nombres

Los solicitantes de certificados no incluirán nombres en las solicitudes que puedan suponer infracción, por el futuro suscriptor, de derechos de terceros.

Bit4id no estará obligada a determinar previamente que un solicitante de certificados tiene derechos de propiedad industrial sobre el nombre que aparece en una solicitud de certificado, sino que en principio procederá a certificarlo.

Asimismo, no actuará como árbitro o mediador, ni de ningún otro modo deberá resolver disputa alguna concerniente a la propiedad de nombres de personas u organizaciones, nombres de dominio, marcas o nombres comerciales.

Sin embargo, en caso de recibir una notificación relativa a un conflicto de nombres, conforme a la legislación del país del suscriptor, podrá emprender las acciones pertinentes orientadas a bloquear, revocar o retirar el certificado emitido.

En todo caso, la entidad de certificación se reserva el derecho de rechazar una solicitud de certificado debido a conflicto de nombres.

Toda controversia o conflicto que se derive del presente documento, se resolverá a través de un Centro de Conciliación, en el marco de la Ley de Conciliación Extrajudicial (Ley 26872). Las partes hacen constar su compromiso de cumplir el laudo que se dicte en el documento contractual que formaliza el servicio.

2.2. Validación inicial de la identidad

La identidad de los suscriptores de certificados se realiza a través de las ER vinculadas a Bit4id. Las Entidades de Registro de acuerdo a sus Declaraciones de Prácticas de Registro, verifican la existencia del

suscriptor mediante su documento oficial de identidad o las escrituras correspondientes, 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, estas se identificarán con su DNI, Carné de Extranjería, Pasaporte o cualquier otro medio de identificación que resulte idóneo en derecho. En aquellos casos en los que se identifiquen personas naturales en certificados cuyo suscriptor sea una persona jurídica, sus identidades podrán alternativamente validarse mediante los registros corporativos de la entidad, empresa u organización de derecho público o privado, suscriptoras de los certificados. El suscriptor producirá una certificación de los datos necesarios, y la remitirá a la Entidad de Registro vinculada de Bit4id, por los medios que ésta habilite, para el registro de la identidad de los firmantes.

2.2.1. Prueba de posesión de clave privada

La posesión de la clave privada se demuestra en virtud del procedimiento fiable de entrega y aceptación del certificado por el suscriptor, en certificados de sello, o por el firmante en certificados de persona natural.

2.2.2. 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, que sean suscriptoras de certificados, podrán actuar como representantes de las mismas, siempre y cuando exista una situación previa de representación legal entre la persona natural y la organización de la que se trate, que exige su reconocimiento por la Entidad de Registro vinculada a Bit4id, la cual se realizará mediante el siguiente procedimiento:

1. El representante del suscriptor acreditará su identidad ante la Entidad de Registro vinculada, acreditando el carácter y facultades que alegue poseer, los cuales de acuerdo a las prácticas de registro de la Entidad de Registro podrán verificar mediante consultas a los registros públicos y/o privados según corresponda.

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: DNI, Carnet de Extranjería, Pasaporte u otro medio 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 del suscriptor, incluyendo los datos relativos a la constitución y personalidad jurídica, o bien el instrumento legal que acredite su existencia.
        - Documento RUC u otro acreditativo de la identificación fiscal de la entidad si aplicase.
    - Los datos relativos a la representación o la capacidad de actuación que ostenta:
        - La vigencia de la representación y extensión de los poderes o la capacidad de actuación (si resulta aplicable).

    El requerimiento de los soportes acreditativos a que se refiere este procedimiento podrá omitirse cuando los datos puedan ser obtenidos por la Entidad de Registro a través de consultas a registros y/o bases de datos públicos y/o privados según corresponda.

3. Las Entidades de Registro vinculadas, comprobarán la identidad del representante mediante la presentación del documento de identidad del que se trate u otro medio idóneo reconocido en derecho para su

identificación, así como el contenido de la representación con la documentación.

4. Las Entidades de Registro vinculadas, verificarán la información suministrada para la autenticación y le devolverá la documentación original si la hubiese aportado.

Las Entidades de Registro de acuerdo a sus prácticas establecerán los flujos para el reconocimiento, pudiendo previa documentación del procedimiento correspondiente delegar parcialmente (si aplica) una o varias actividades relativas a la identificación y/o registro de suscriptores y firmantes identificados en los certificados, siempre bajo su responsabilidad.

La prestación del servicio de certificación se formaliza mediante el oportuno contrato entre Bit4id y el suscriptor. Los contratos entre Bit4id y los suscriptores podrán ser firmados en forma digital o manuscritamente de acuerdo con lo previsto en normativa aplicable.

2.2.3. 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, que podrá ser desarrollado por las Entidades de Registro vinculadas a Bit4id, de acuerdo a los distintos modelos de gestión y organización de sus clientes, dentro de los límites de la normativa aplicable.

2.2.3.1. En los certificados

La identidad de las personas naturales firmantes identificados en los certificados, se valida a través de sus documentos oficiales de identificación (Documento Nacional de Identidad, carné de extranjería, 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, podrá ser validada comparando la información de la solicitud con los registros internos de la entidad, empresa u organización de derecho público o privado a la que está vinculado, o bien con la documentación que ésta haya suministrado sobre la persona natural que identifica como firmante, asegurando la corrección de la información a certificar.

2.2.3.2. Validación de la Identidad

Para la solicitud de certificados, la Entidad de Registro vinculada valida la identidad de la persona natural solicitante, acreditada a través de su DNI, Carné de Extranjería, Pasaporte u otro medio idóneo reconocido en derecho para su identificación.

Para la solicitud de los certificados cuyo suscriptor sea una persona jurídica se requerirá la identificación del representante del suscriptor autorizado al momento de formular la solicitud debido a la relación ya acreditada entre la persona natural y entidad, empresa u organización de derecho público o privado a la que está vinculada. Sin embargo, antes de la entrega de un certificado, la entidad, empresa u organización de derecho público o privado suscriptora, por medio de su responsable de certificación, de tenerlo, u otro miembro designado, deberá contrastar la identidad de la persona natural identificada en el certificado mediante su presencia natural.

Durante este trámite se confirma la identidad de la persona natural identificada en el certificado. Por este motivo, en todos los casos en que se expide un certificado se acredita ante la entidad de registro la identidad de la persona natural firmante.

La Entidad de Registro de acuerdo a sus prácticas de registro, verificará mediante la exhibición de documentos o a través de sus propias fuentes de información, el resto de datos y atributos a incluir en el certificado, guardando documentación acreditativa de la validez de estos.

2.2.3.3. 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, el contrato mercantil que lo vincula, o el acta donde se indique su cargo, o la solicitud como miembro de la organización etc…) de cada una de las personas públicas y privadas a las que están vinculadas.

2.2.4. Información de suscriptor no verificada

Bit4id no incluye ninguna información de suscriptor no verificada en los certificados.

2.2.5. Autenticación de la identidad de una ER y sus operadores

Para la vinculación de una nueva Entidad de Registro, Bit4id realiza las verificaciones necesarias para confirmar la existencia de la entidad u organización de la que se trate. Para ello, Bit4id se asegurará de que la Entidad de Registro consta debidamente acreditada y registrada ante la Autoridad Administrativa Competente, o que lo esté antes del inicio de la prestación de dichos servicios.

2.3. Identificación y autenticación de solicitudes de renovación

2.3.1. Validación para la renovación rutinaria de certificados

La Entidad de Registro vinculada a Bit4id, comprueba la identidad del solicitante de la re-emisión del certificado a través de métodos varios, de acuerdo a las prácticas de registro de la Entidad de Registro de la que se trate. A título meramente ilustrativo y no taxativo se mencionan algunos:

- El uso del código "CRE" o "ERC" relativo al certificado anterior, o de otros métodos de autenticación personal, que consiste en información que sólo conoce la persona natural identificada en el certificado, y que le permite renovar de forma automática sin tener que apersonarse ante la Entidad de Registro su certificado, en el marco de la legislación aplicable.

- A través del empleo del certificado vigente para su re-emisión.

Las Entidades de Registro deben verificar la información que ha sido aportada por el solicitante para la emisión inicial del certificado, a fin de verificar si sigue siendo válida. Si cualquier información del suscriptor o de la persona natural identificada en el certificado ha cambiado, se registrará adecuadamente la nueva información de acuerdo con las formas y métodos previstos en este Documento.

2.3.2. Identificación y autenticación de la solicitud de re-emisión

Las Entidades de Registro vinculadas a Bit4id , verificarán la identidad, en cuyo caso se aplicará lo dispuesto en la sección anterior.

La re-emisión 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.

Los suscriptores y/o firmantes del certificado podrán solicitar la re-emisión del mismo utilizando medios telemáticos, identificándose y/o firmando digitalmente la correspondiente solicitud con certificado digital válido.

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

Bit4id, un operador o personal autorizado de la Entidad de Registro vinculada a Bit4id, 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:
  - Identificándose y autenticándose mediante el uso del Código de Revocación (ERC o ERC) a través de la página web en horario 24x7.
  - Identificándose mediante el uso de certificado digital válido.
  - 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 Bit4id y/o Entidades de Registro vinculadas a esta.
- Las Entidades de Registro vinculadas a Bit4id: deberán identificar al firmante ante una petición de revocación, suspensión o reactivación según los propios medios que considere necesarios. En los casos en que la solicitud de revocación se realice por un tercero distinto al suscriptor, este tercero deberá apersonarse en la Entidad de Registro.

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

Los procedimientos que se refieren a la gestión del ciclo de vida de los certificados y en general cuantas actuaciones sean inherentes a los servicios propios de la Entidad de Registro, éstos serán descritos en el documento de Declaración de Prácticas de Registro de las entidades vinculadas a Bit4id.

3.1. Solicitud de emisión de certificado

3.1.1. Legitimación para solicitar la emisión

Los procedimientos relativos a la Entidad de Registro se encuentran disponibles en los documentos de Declaración de Prácticas de Registro de las entidades vinculadas a Bit4id, disponible en la siguiente página web: https://web.uanataca.com/pe.

3.1.2. Procedimiento de alta y responsabilidades

Los procedimientos relativos a la Entidad de Registro se encuentran disponibles en los documentos de Declaración de Prácticas de Registro de las entidades vinculadas a Bit4id, disponibles en la siguiente página web:https://web.uanataca.com/pe.

3.2. Procesamiento de la solicitud de certificación

3.2.1. Ejecución de las funciones de identificación y autenticación

Los procedimientos relativos a la Entidad de Registro se encuentran disponibles en los documentos de Declaración de Prácticas de Registro de las entidades vinculadas a Bit4id, disponibles en la siguiente página web: https://web.uanataca.com/pe.

3.2.2. Aprobación o rechazo de la solicitud

Los procedimientos relativos a la Entidad de Registro se encuentran disponibles en los documentos de Declaración de Prácticas de Registro de las entidades vinculadas a Bit4id, disponibles en la siguiente página web: https://web.uanataca.com/pe.

3.2.3. Plazo para resolver la solicitud

Los procedimientos relativos a la Entidad de Registro se encuentran disponibles en los documentos de Declaración de Prácticas de Registro de las entidades vinculadas a Bit4id, disponibles en la siguiente página web: https://web.uanataca.com/pe.

3.3. Emisión del certificado

3.3.1. Acciones de la EC durante el proceso de emisión

Los procedimientos relativos a la Entidad de Registro se encuentran disponibles en el documento de Declaración de Prácticas de Registro de las entidades vinculadas a Bit4id, disponibles en la siguiente página web: https://web.uanataca.com/pe.

3.3.2. Notificación de la emisión al suscriptor

Los procedimientos relativos a la Entidad de Registro se encuentran disponibles en los documentos de Declaración de Prácticas de Registro de las entidades vinculadas a Bit4id, disponibles en la siguiente página web: https://web.uanataca.com/pe.

3.4. Entrega y aceptación del certificado

3.4.1. Conducta que constituye aceptación del certificado

Los procedimientos relativos a la Entidad de Registro se encuentran disponibles en los documentos de Declaración de Prácticas de Registro de las entidades vinculadas a Bit4id, disponibles en la siguiente página web: https://web.uanataca.com/pe.

3.4.2. Publicación del certificado por la EC

Los procedimientos relativos a la Entidad de Registro se encuentran disponibles en los documentos de Declaración de Prácticas de Registro de las entidades vinculadas a Bit4id, disponibles en la siguiente página web: https://web.uanataca.com/pe.

3.4.3. Notificación de la emisión a terceros

Los procedimientos relativos a la Entidad de Registro se encuentran disponibles en los documentos de Declaración de Prácticas de Registro de las entidades vinculadas a Bit4id, disponibles en la siguiente página web: https://web.uanataca.com/pe.

3.5. Uso del par de claves y del certificado

3.5.1. Uso por el firmante

El firmante se obliga a:

- Facilitar a la Entidad de Registro información completa y adecuada, conforme a los requisitos de este Documento, 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 este documento.
- Ser especialmente diligente en la custodia de su clave privada, con el fin de evitar usos no autorizados, de acuerdo con lo establecido en esta Declaración de Prácticas.
- Comunicar a las Entidades 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 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 una vez transcurrido el periodo de vigencia o duración del certificado.

Bit4id obliga con el firmante 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 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 una entidad 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

Bit4id obliga contractualmente al suscriptor a:

- Facilitar a la Entidad de Certificación información completa y adecuada, conforme a los requisitos de su 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 su Declaración de Prácticas de Certificación.
- Comunicar a Bit4id , Entidades 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 las mismas.
- No monitorizar, manipular o realizar actos de ingeniería reversa sobre la implantación técnica de los servicios de certificación de Bit4id, sin permiso previo por escrito.
- No comprometer la seguridad de los servicios de certificación de Bit4id como Entidad de Certificación.

3.5.2.2. Responsabilidad civil del suscriptor de certificado

Bit4id 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

Bit4id 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.

- 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 de Bit4id, sin permiso previo por escrito.
- No comprometer la seguridad de los servicios de certificación de Bit4id como Entidad de Certificación.

3.5.3.2. Responsabilidad civil del tercero que confía en certificados

Bit4id 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, por lo que debe atenderse a lo establecido en la sección 3.7.

3.7. Renovación de claves

3.7.1. Circunstancias para la renovación

Los certificados vigentes se pueden renovar mediante un procedimiento específico y simplificado de solicitud, al efecto de mantener la continuidad del servicio de certificación. Los procedimientos relativos a la Entidad de Registro se encuentran disponibles en los documentos de Declaración de Prácticas de Registro de las entidades vinculadas a Bit4id, disponibles en la siguiente página web: https://web.uanataca.com/pe.

3.7.2. Personas habilitadas para solicitar la renovación

Los procedimientos relativos a la Entidad de Registro se encuentran disponibles en los documentos de Declaración de Prácticas de Registro de las entidades vinculadas a Bit4id, disponibles en la siguiente página web: https://web.uanataca.com/pe. Los procedimientos de la Entidad de Registro se realizarán dentro de los límites de su Declaración de Prácticas de Certificación.

3.7.3. Procesamiento de las solicitudes para la renovación

Los procedimientos relativos a la Entidad de Registro se encuentran disponibles en los documentos de Declaración de Prácticas de Registro de las entidades vinculadas a Bit4id, disponibles en la siguiente página web: https://web.uanataca.com/pe.

3.8. Modificación de certificados

La modificación de certificados, excepto la modificación de la clave pública certificada, que se considera renovación, será tratada como una nueva emisión de certificado.

3.9. 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.

3.9.1. Causas de revocación de certificados

Como norma general, se procederá a la revocación de un certificado cuando concurra alguna de las siguientes causas:

1) Circunstancias que afectan a la información contenida en el certificado:
   a) Modificación de alguno de los datos contenidos en el certificado, después de la correspondiente emisión del certificado que incluye las modificaciones.
   b) Descubrimiento de que alguno de los datos contenidos en la solicitud de certificado es incorrecto.
   c) Descubrimiento de que alguno de los datos contenidos en el certificado es incorrecto.

2) Circunstancias que afectan a la seguridad de la clave o del certificado:
   a) Compromiso de la clave privada, de la infraestructura o de los sistemas de la Entidad de Certificación digital que emitió el certificado, siempre que afecte a la fiabilidad de los certificados emitidos a partir de ese incidente.
   b) Infracción, por la Entidad de Certificación o la Entidad de Registro, de los requisitos previstos en los procedimientos de gestión de certificados, establecidos en su Declaración de Prácticas de Certificación.

c) Compromiso o sospecha de compromiso de la seguridad de la clave o del certificado emitido.
d) Acceso o utilización no autorizados, por un tercero, de la clave privada correspondiente a la clave pública contenida en el certificado.
e) El uso irregular del certificado por la persona natural identificada en el certificado, o la falta de diligencia en la custodia de la clave privada.

3) Circunstancias que afectan al suscriptor o a la persona natural identificada en el certificado:
   a) Finalización de la relación jurídica de prestación de servicios entre Bit4id y el suscriptor.
   b) Modificación o extinción de la relación jurídica subyacente o causa que provocó la emisión del certificado a la persona natural identificada en el certificado.
   c) Infracción por el solicitante del certificado de los requisitos preestablecidos para la solicitud de este.
   d) Infracción por el suscriptor o por la persona identificada en el certificado, de sus obligaciones, responsabilidad y garantías, establecidas en el documento jurídico correspondiente.
   e) La incapacidad sobrevenida o el fallecimiento del poseedor de claves.
   f) La extinción de la persona jurídica suscriptora del certificado, así como el fin de la autorización del suscriptor al poseedor de claves o la finalización de la relación entre suscriptor y persona identificada en el certificado.
   g) Solicitud del suscriptor de revocación del certificado.

4) Circunstancias que afectan a la seguridad del dispositivo de creación de firma
   a. Compromiso o sospecha de compromiso de la seguridad del dispositivo criptográfico.
   b. Pérdida o inutilización por daños del dispositivo de creación de firma.

c. Acceso no autorizado, por un tercero, a los datos de activación del Firmante o del responsable de certificado.

5) Otras circunstancias:
   a) La terminación del servicio de certificación de la Entidad de Certificación.
   b) El uso del certificado que sea dañino y continuado para la Entidad de Certificación. En este caso, se considera que un uso es dañino en función de los siguientes criterios:
      - La naturaleza y el número de quejas recibidas.
      - La identidad de las entidades que presentan las quejas.
      - La legislación relevante vigente en cada momento.
      - La respuesta del suscriptor o de la persona identificada en el certificado a las quejas recibidas.

3.9.2. Causas de suspensión de un certificado

Los certificados de Bit4id, pueden ser suspendidos a partir de las siguientes causas:

- Cuando así sea solicitado por el suscriptor o la persona natural identificada en el certificado.
- Cuando la documentación requerida en la solicitud de revocación sea suficiente pero no se pueda identificar razonablemente al suscriptor o la persona natural identificada en el certificado.
- La falta de uso del certificado durante un periodo prolongado de tiempo, conocido previamente.
- Si se sospecha el compromiso de una clave, hasta que éste sea confirmado. En este caso, Bit4id tiene que asegurarse de que el certificado no está suspendido durante más tiempo del necesario para confirmar su compromiso.

3.9.3. Causas de reactivación de un certificado

Los certificados de Bit4id pueden ser reactivados a partir de las siguientes causas:

- Cuando el certificado se encuentre en un estado de suspendido.
- Cuando así sea solicitado por el suscriptor o la persona natural identificada en el certificado.

3.9.4. Quién puede solicitar la revocación, suspensión o reactivación

Pueden solicitar la revocación, suspensión o reactivación de un certificado:

- La persona identificada en el certificado.
- El suscriptor del certificado por medio de su representante legal o agente debidamente autorizado.

3.9.5. Procedimientos de solicitud de revocación, suspensión o reactivación

Los procedimientos relativos a la Entidad de Registro se encuentran disponibles en el documento de Declaración de Prácticas de Registro de las entidades vinculadas a Bit4id, disponibles en la siguiente página web: https://web.uanataca.com/pe.

No obstante lo anterior, la entidad que precise revocación, suspensión o reactivación de un certificado, puede solicitarlo directamente a Bit4id, a la Entidad de Registro del suscriptor o realizarlo él mismo a través del servicio online disponible en la página web. 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 para la petición de revocación.

La solicitud debe ser autenticada, por Bit4id, de acuerdo con los requisitos establecidos en este documento, antes de proceder a la revocación, suspensión o reactivación.

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

El servicio de gestión de revocación y el servicio de consulta son considerados servicios críticos.

3.9.6. Plazo temporal de solicitud de revocación, suspensión o reactivación

Las solicitudes de revocación, suspensión o reactivación se remitirán de forma inmediata en cuanto se tenga conocimiento.

3.9.7. Plazo temporal de procesamiento de la solicitud de revocación, suspensión o reactivación

Los procedimientos relativos a la Entidad de Registro se encuentran disponibles en los documentos de Declaración de Prácticas de Registro de las entidades vinculadas a Bit4id, disponibles en la siguiente página web: https://web.uanataca.com/pe.

Cuando la petición se haya realizado directamente ante la Entidad de Certificación, Bit4id procesará las peticiones dentro de las 24 horas siguientes a la realización de esta.

3.9.8. 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 UANATACA.

Las Listas de Revocación de Certificados se publican en el repositorio disponible en la siguiente web: https://web.uanataca.com/pe, así como en las siguientes direcciones web, indicadas dentro de los certificados:

- http://crl1.uanataca.com/public/pki/crl/CA1subordinada.crl
- http://crl2.uanataca.com/public/pki/crl/CA1subordinada.crl
- 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/

3.9.9. Frecuencia de emisión de listas de revocación de certificados (LRCs)

Bit4id emite una LRC al menos cada 24 horas.

La LRC indica el momento programado de emisión de una nueva LRC, si bien se puede emitir una LRC antes del plazo indicado en la LRC anterior, para reflejar revocaciones.

La LRC mantiene obligatoriamente el certificado revocado o suspendido hasta que expira.

3.9.10. Plazo máximo de publicación de LRCs

Las LRCs se publican en el Depósito en un periodo inmediato razonable tras su generación, que en ningún caso no supera unos pocos minutos.

3.9.11. Disponibilidad de servicios de comprobación en línea de estado de certificados

De forma alternativa, los terceros que confían en certificados podrán consultar el Depósito de certificados de Bit4id, que se encuentra disponible las 24 horas de los 7 días de la semana en el web https://web.uanataca.com/pe.

Para comprobar la última CRL emitida, deberán descargarse la que corresponda a cada CA, en concreto:

- *Autoridad de Certificación Raíz (UANATACA ROOT 2016):*
  - http://crl1.uanataca.com/public/pki/crl/arl_uanataca.crl
  - http://crl2.uanataca.com/public/pki/crl/arl_uanataca.crl

- *Autoridad de Certificación Intermedia 1 (UANATACA CA1 2016)*
  - http://crl1.uanataca.com/public/pki/crl/CA1subordinada.crl
  - http://crl2.uanataca.com/public/pki/crl/CA1subordinada.crl

- *Autoridad de Certificación Intermedia 2 (UANATACA CA2 2016):*
  - http://crl1.uanataca.com/public/pki/crl/CA2subordinada.crl
  - http://crl2.uanataca.com/public/pki/crl/CA2subordinada.crl

En caso de fallo de los sistemas de comprobación de estado de certificados por causas fuera del control de Bit4id, se realizarán los mayores esfuerzos posibles para asegurar que este servicio se mantenga inactivo el mínimo tiempo posible, que no podrá superar un día.

Bit4id suministra información a los terceros que confían en certificados acerca del funcionamiento del servicio de información de estado de certificados.

3.9.12. 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.

3.9.13. Requisitos especiales en caso de compromiso de la clave privada

El compromiso de la clave privada de Bit4id Entidad de Certificación es notificado a todos los participantes en los servicios de certificación, en la medida de lo posible, mediante la publicación de este hecho en la página web, así como, si se considera necesario, en otros medios de comunicación, incluso en papel.

De igual manera, Bit4id pondrá a disposición de todos los usuarios mediante su página web, la publicación en caso de compromiso de su clave privada.

3.9.14. Período máximo de un certificado digital en estado suspendido

El plazo máximo de un certificado digital en estado suspendido es indefinido hasta su caducidad.

3.10. Finalización de la suscripción

Transcurrido el periodo de vigencia del certificado o si este es revocado previamente a esta fecha, finalizará la suscripción al servicio.

Como excepción, el suscriptor puede mantener el servicio vigente, de acuerdo a las previsiones de la sección 4.7 de su Declaración de Prácticas de Certificación. Bit4id puede emitir de oficio un nuevo certificado, mientras los suscriptores mantengan dicho estado.

3.11. Depósito y recuperación de claves

3.11.1. Política y prácticas de depósito y recuperación de claves

Bit4id no presta servicios de depósito y recuperación de claves.

3.11.2. Política y prácticas de encapsulado y recuperación de claves de sesión

Sin estipulación.

3.12. Generación e instalación del par de claves

3.12.1. Generación del par de claves

El par de claves de las entidades de certificación intermedias "UANATACA CA1 2016" y "UANATACA CA2 2016" son creadas por la entidad de certificación raíz "UANATACA ROOT 2016" de acuerdo con las políticas y procedimientos de ceremonia de UANATACA, S.A., dentro del perímetro de alta seguridad destinado a esta tarea.

Las actividades realizadas durante la ceremonia de generación de claves han sido registradas, fechadas y firmadas por todos los individuos participantes en la misma, con la presencia de un Auditor. Dichos registros son custodiados a efectos de auditoría y seguimiento durante un período apropiado determinado.

Para la generación de la clave de las entidades de certificación raíz e intermedia se utilizan dispositivos con las certificaciones FIPS 140-2 level 3 y Common Criteria EAL4+.

UANATACA ROOT 2016	4.096 bits	25 años
UANATACA CA1 2016	4.096 bits	13 años
- Certificados de entidad final	2.048 bits	Hasta 3 años
UANATACA CA2 2016	4.096 bits	13 años

- Certificados de la Unidad de Sello de tiempo	2.048 bits	Hasta 8 años

3.12.1.1. Generación del par de claves del firmante

Las claves del firmante pueden ser generadas por él mismo mediante dispositivos hardware y/o software autorizados.

Las claves son generadas usando el algoritmo de clave pública RSA, con una longitud mínima de 2048 bits.

3.12.2. Envío de la clave privada al firmante

En certificados en dispositivo de creación de firma la clave privada se genera y se almacena debidamente protegida en el interior de dicho dispositivo cualificado.

En certificados en software la clave privada la genera el mismo firmante y se almacena en el sistema informático del firmante, por lo que en este caso no existe envío de clave privada, garantizando el control exclusivo de la clave por parte del usuario

En certificados emitidos dentro de HSM la clave privada del firmante se genera en un área privada del firmante en un HSM. Las credenciales de acceso a la clave privada son introducidas por el propio firmante, no siendo almacenadas ni susceptibles de capacidad de deducción o intercepción por el sistema de generación y custodia remota. La clave privada no se envía al firmante, es decir, nunca abandona el entorno de seguridad que garantiza el control exclusivo de la clave privada por parte del firmante.

3.12.3. Envío de la clave pública al emisor del certificado

El método de remisión de la clave pública a la Entidad de Certificación digital es PKCS#10, otra prueba criptográfica equivalente o cualquier otro método aprobado.

3.12.4. Distribución de la clave pública de la Entidad de Certificación

Las claves de la Entidad de Certificación son comunicadas a los terceros que confían en certificados, asegurando la integridad de la clave y autenticando su origen, mediante su publicación en el Depósito.

Los usuarios pueden acceder al Depósito para obtener las claves públicas, y adicionalmente, en aplicaciones S/MIME, el mensaje de datos puede contener una cadena de certificados, que de esta forma son distribuidos a los usuarios.

El certificado de las Autoridades de Certificación Raíz y de las Subordinadas estará a disposición de los usuarios en la página web.

3.12.5. Tamaños de claves

- La longitud de las claves de la Autoridad de Certificación raíz es de 4096 bits.
- La longitud de las claves de las Autoridades de Certificación subordinadas es de 4096 bits.
- La longitud de las claves de los Certificados de Entidad final es de 2048 bits.

3.12.6. Generación de parámetros de clave pública

La clave pública de la Autoridades de Certificación raíz, subordinadas y de los certificados de los suscriptores está codificada de acuerdo con RFC 5280.

3.12.7. Comprobación de calidad de parámetros de clave pública

- Longitud del Módulo = 4096 bits
- Algoritmo de generación de claves: rsagen1
- Funciones criptográficas de Resumen: SHA256.

3.12.8. Generación de claves en aplicaciones informáticas o en bienes de equipo

Todas las claves se generan en bienes de equipo, de acuerdo con lo indicado en la sección 6.1.1.

3.12.9. Propósitos de uso de claves

Los usos de las claves para los certificados de las CA son exclusivamente para la firma de certificados y de LCRs.

Los usos de las claves para los certificados de entidad final son exclusivamente para la firma digital y el no repudio.

3.13. Protección de la clave privada

3.13.1. Estándares de módulos criptográficos

En relación a los módulos que gestionan claves de la Entidad de Certificación y de los suscriptores de certificados de firma digital, se asegura el nivel exigido por los estándares indicados en las secciones anteriores.

3.13.2. Control por más de una persona (n de m) sobre la clave privada

Se requiere un control multi-persona para la activación de la clave privada de la AC. En el caso de su Declaración de Prácticas de Certificación, en concreto existe una política de **3 de 6** personas para la activación de las claves.

Los dispositivos criptográficos se encuentran protegidos físicamente tal y como se determina en este documento.

3.13.3. Depósito de la clave privada

La Entidad de Certificación no almacena copias utilizables por medios propios de las claves privadas de los firmantes.

3.13.4. Copia de respaldo de la clave privada

Se realiza copia de backup de las claves privadas de las CA que hacen posible su recuperación en caso de desastre, de pérdida o deterioro de las mismas. Tanto la generación de la copia como la recuperación de ésta necesitan al menos de la participación de dos personas.

Estos ficheros de recuperación se almacenan en armarios ignífugos y en el centro de custodia externo.

Claves generadas en dispositivo software: la Entidad de Certificación no puede realizar backups de las claves, ya que no dispone de acceso a las mismas. El firmante sí que puede realizar un backup.

Claves generadas en dispositivos criptográficos seguros de creación de firma: no se puede realizar backups de las claves, ya que no es posible su exportación desde el mismo.

Claves generadas en HSM: Sólo es posible realizar backups de un bloob cifrado con la clave Security World del HSM utilizado, siendo imposible su descifrado sin el uso de las credenciales que sólo el titular del certificado conoce.

3.13.5. Archivo de la clave privada

Las claves privadas de las AC son archivadas por un periodo de **10 años** después de la emisión del último certificado. Se almacenarán en archivos

ignífugos seguros y en el centro de custodia externo. Al menos será necesaria la colaboración de dos personas para recuperar la clave privada de las AC en el dispositivo criptográfico inicial.

La Entidad de Certificación no genera ni archiva claves de certificados, emitidas en software.

3.13.6. Introducción de la clave privada en el módulo criptográfico

Las claves privadas se generan directamente en los módulos criptográficos.

3.13.7. Método de activación de la clave privada

Las claves privadas de la Entidad de Certificación se almacenan cifradas en los módulos criptográficos.

3.13.8. Método de desactivación de la clave privada

La clave privada se activa mediante la ejecución del correspondiente procedimiento de inicio seguro del módulo criptográfico, por las personas indicadas en la sección 3.13.2.

Las claves de la AC se activan por un proceso de m de n (3 de 6).

La activación de las claves privadas de la AC Intermedia es gestionada con el mismo proceso de m de n que las claves de la AC.

3.13.9. Método de destrucción de la clave privada

Para la desactivación de la clave privada se seguirán los pasos descritos en el manual del administrador del equipo criptográfico correspondiente.

3.13.10. Clasificación de módulos criptográficos

Con anterioridad a la destrucción de las claves, se emitirá una revocación del certificado de las claves públicas asociadas a las mismas.

Se destruirán físicamente o reiniciarán a bajo nivel los dispositivos que tengan almacenada cualquier parte de las claves privadas de la Autoridad de Certificación. Para la eliminación se seguirán los pasos descritos en el manual del administrador del equipo criptográfico.

Finalmente se destruirán de forma segura las copias de seguridad.

Las claves del firmante en software se podrán destruir mediante el borrado de las mismas, siguiendo las instrucciones de la aplicación que las alberga.

Las claves del firmante en hardware podrán ser destruidas mediante una aplicación informática especial.

3.13.11. Clasificación de módulos criptográficos

Ver la sección 3.13.1.

3.14. Otros aspectos de gestión del par de claves

3.14.1. Archivo de la clave pública

Bit4id archiva sus claves públicas de forma rutinaria, de acuerdo con lo establecido en la sección **¡Error! No se encuentra el origen de la referencia.** de este documento.

3.14.2. Períodos de utilización de las claves pública y privada

Los periodos de utilización de las claves son los determinados por la duración del certificado, transcurrido el cual no pueden continuar utilizándose.

4. Perfiles de certificados y listas de certificados revocados

4.1. Perfil de certificado

Todos los certificados emitidos bajo esta política cumplen con el estándar X.509 versión 3 y el RFC 3739 y los diferentes perfiles descritos en la norma EN 319 412.
La documentación relativa a los perfiles puede solicitarse a Bit4id.

4.1.1. Número de versión

Bit4id emite certificados X.509 Versión 3.

4.1.2. Extensiones del certificado

Las extensiones de los certificados se encuentran detalladas en los documentos de perfiles que son accesibles desde la siguiente página web: https://web.uanataca.com/pe.

De esta forma se permite mantener unas versiones más estables de la Declaración de Prácticas de Certificación y desligarlos de los frecuentes ajustes en los perfiles.

4.1.3. 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

4.1.4. Formato de Nombres

Los certificados deberán contener las informaciones que resulten necesarias para su uso, según determine la correspondiente política.

4.1.5. Restricción de los nombres

Los nombres contenidos en los certificados están restringidos a "Distinguished Names" X.500, que son únicos y no ambiguos.

4.1.6. Identificador de objeto (OID) de los tipos de certificados

Todos los certificados incluyen un identificador de política de certificados bajo la que han sido emitidos, de acuerdo con la estructura indicada en este documento.

4.2. Perfil de la lista de revocación de certificados

4.2.1. Número de versión

Las CRL emitidas por Bit4id son de la versión 2.

4.2.2. Perfil de OCSP

Según el estándar IETF RFC 6960.

5. Anexo I.- Definiciones y acrónimos

AAC	Autoridad Administrativa Competente
AC	Autoridad de Certificación
CA	Certification Authority. Autoridad de Certificación
CP	Certificate Policy. Políticas de Certificación
CPD	Centro de Procesacimiento de Datos.
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
DCCF	Dispositivo Cualificado de Creación de Firma
DN	Distinguished Name. Nombre distintivo dentro del certificado digital
DSA	Digital Signature Algorithm. Estándar de algoritmo de firma
EC	Entidad de certificación
ER	Entidad de Registro o Verificación
ERC	Código de Revocación
FIPS	Federal Information Processing Standard Publication
HSM	Hardware Security Module. Módulo de Seguridad Hardware
IOFE	Infraestructura Oficial de Firma Electrónica
ISO	International Organization for Standardization. Organismo Internacional de Estandarización
LDAP	Lightweight Directory Access Protocol. Protocolo de acceso a directorios
LRC	Listas de revocación de certificados
NTP	Network Time Protocol (NTP
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
PDS	Policy Disclosure Statements. Textos de divulgación
PIN	Personal Identification Number. Número de identificación personal
PKI	Public Key Infrastructure. Infraestructura de llave pública
QSCD	Qualified Signature Creation Device. Dispositivo Cualificado de Creación de Firma
RA	Autoridad de Registro
ROA	Real Instituto y Observatorio de la Armada
RPS	Declaración de prácticas de registro o verificación
RSA	Rivest-Shimar-Adleman. Tipo de algoritmo de cifrado
RUC	Registro Único de Contribuyentes
SHA	Secure Hash Algorithm. Algoritmo seguro de Hash
SSL	Secure Sockets Layer
TCP/IP	Transmission Control. Protocol/Internet Protocol