BIT4ID SAC

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN

Información general

Control documental

Clasificación de seguridad:	Público
Entidad de destino:	BIT4ID SAC
Versión:	2.0
Fecha edición:	11/05/2020
Fichero:	BIT4IDSAC_DPC_v2
Formato:	Office

Estado formal

Preparado por:	Revisado por:	Aprobado por:
Nombre: Alejandro Grande Fecha: 11/05/2020	Nombre: Albert Borrás Fecha: 11/05/2020	Nombre: Jorge García Fecha: 12/05/2020

Control de versiones

Versión	Partes que cambian	Descripción del cambio	Autor del cambio	Fecha del cambio
1.0	Original	Creación del documento	ABD/DMP	16/11/2017
1.1	1.6, 3.1 y 6.11	Ajuste de los perfiles de certificados Se ha agregado el protocolo de comunicación entre la ER y la EC	ABD	27/04/2018
1.2	7.1.4, 7.1.6, 7.2.2,	Ajustes conformes al Anexo I de la guía de Acreditación de EC	ABD	30/04/2018
1.3	1.4 y 7.2.1 4.3.1 y 4.3.2 5.8.2	Subsanación de errores. Se ha definido correctamente el proceso de emisión de certificado definido en el apartado 4.3. Se redefinido el procedimiento de cese.	ABD	06/03/2020
2	Completo	Ajuste de la terminología aplicada en la versión original del documento, así como modificación del formato, para adaptar a las necesidades del ente regulador.	AGB	11/05/2020

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 las prácticas de certificación de firma digital 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 "Declaración de Prácticas de Certificación de Bit4id".

1.3.1. Identificadores de certificados

Bit4idha 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*

En caso de contradicción entre esta Declaración de Prácticas de Certificación y otros documentos de prácticas y procedimientos, prevalecerá lo establecido en esta Declaración de Prácticas.

1.4. Definiciones y Acrónimos

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.

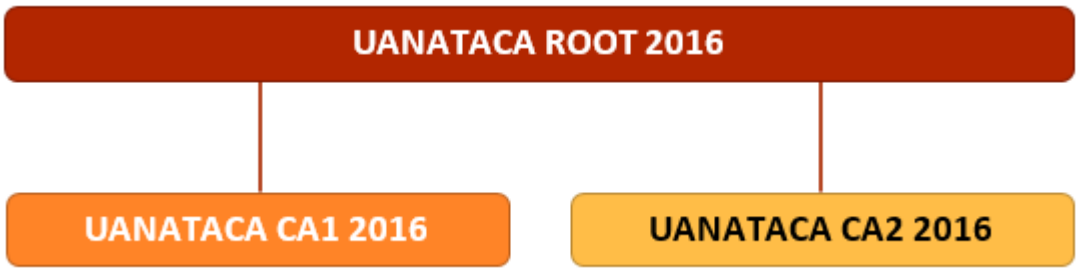
Más información en el ANEXO 1 del presente documento.

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.

Bit4id formalizará 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 esta Declaración de Prácticas de Certificación, 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)
c. Key Encipherment

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)
c. Key Encipherment

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)
c. Key Encipherment

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)
    c. Key Encipherment

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 Declaración de Prácticas de Certificación, 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.

Bit4idno 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 esta Declaración de Prácticas de Certificación, 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.

1.7. Persona de Contacto

1.7.1. Datos de la Entidad de Certificación

Nombre: Bit4id S.A.C
Dirección: Av. Antonio Miroquesada 360 – piso 04 Ofic. 112
Magdalena del Mar
15076 – Lima
Correo electrónico: info.pe@uanataca.com
Página web: https://web.uanataca.com/pe

1.7.2. Datos de la Entidad de Registro

Nombre: Bit4id S.A.C
Dirección: Av. Antonio Miroquesada 360 – piso 04 Ofic. 112
Magdalena del Mar
15076 – Lima
Correo electrónico: info.pe@uanataca.com
Página web: https://web.uanataca.com/pe

1.8. Administración de la política

1.8.1. Organización que administra el documento

Nombre: Bit4id S.A.C
Dirección: Av. Antonio Miroquesada 360 – piso 04 Ofic. 112
Magdalena del Mar, 15076 – Lima
Correo electrónico: info.pe@uanataca.com
Página web: https://web.uanataca.com/pe
Responsable Administrador del Documento: Jorge García Aliaga

1.8.2. Datos de contacto de la organización

Nombre: Bit4id S.A.C
Dirección: Av. Antonio Miroquesada 360 – piso 04 Ofic. 112
Magdalena del Mar, 15076 – Lima
Correo electrónico: info.pe@uanataca.com
Página web: https://web.uanataca.com/pe
Persona de contacto: Jorge García Aliaga

1.8.3. Procedimientos de gestión del documento

El sistema documental y de organización de Bit4id garantiza, mediante la existencia y la aplicación de los correspondientes procedimientos, el correcto mantenimiento de este documento y de las especificaciones de servicio relacionados con el mismo.

2. Publicación de información y depósito de certificados

2.1. Depósito(s) de certificados

Bit4id a través de la infraestructura tecnológica mediante la cual presta sus servicios como Entidad de Certificación, dispone de un Depósito de certificados, en el que se publican las informaciones relativas a los servicios de certificación.

Dicho servicio se encuentra disponible durante las 24 horas de los 7 días de la semana y, en caso de fallo del sistema fuera de control de Bit4id, se realizarán los mejores esfuerzos para que el servicio se encuentre disponible de nuevo en el plazo establecido en la sección 5.7.4 de esta Declaración de Prácticas de Certificación.

Del mismo modo, Bit4id dispone y gestiona su propio repositorio en el que se recogen toda la documentación relevante y propia de una Entidad de Certificación. Todo ello publicado en la siguiente dirección: https://web.uanataca.com/pe.

2.2. Publicación de información la Entidad de Certificación

Bit4id a través de la plataforma de información, publica las siguientes informaciones, en su Depósito:

- Declaración de Prácticas de Certificación.
- Las Políticas de los Certificados aplicables.
- Las Entidades de Registro Vinculadas.
- Los certificados emitidos, cuando se haya obtenido consentimiento de la persona natural identificada en el certificado.
- Las listas de certificados revocados y otras informaciones de estado de revocación de los certificados.

2.3. Frecuencia de publicación

La información de la Entidad de Certificación, incluyendo las políticas y la Declaración de Prácticas de Certificación, se publica en cuanto se encuentra disponible.

Los cambios en la Declaración de Prácticas de Certificación se rigen por lo establecido en la sección 1.8 de este documento.

La información de estado de revocación de certificados se publica de acuerdo con lo establecido en las secciones 4.9.9 y 4.9.10 de esta Declaración de Prácticas de Certificación.

2.4. Control de acceso

Bit4id no limita el acceso de lectura a las informaciones establecidas en la sección 2.2, pero establece controles para impedir que personas no autorizadas puedan añadir, modificar o borrar registros del Depósito, para proteger la integridad y autenticidad de la información, especialmente la información de estado de revocación.

Por ello se emplean sistemas fiables para el Depósito, de modo tal que:

- Únicamente personas autorizadas puedan hacer anotaciones y modificaciones.
- Pueda comprobarse la autenticidad de la información.
- Los certificados sólo estén disponibles para consulta si la persona natural identificada en el certificado ha prestado su consentimiento.
- Pueda detectarse cualquier cambio técnico que afecte a los requisitos de seguridad.

3. Identificación y autenticación

3.1. Registro inicial

3.1.1. 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.

3.1.1.1. Certificados de PERSONAS

3.1.1.1.1. 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.

3.1.1.2. Certificados de Persona Jurídica

3.1.1.2.1. 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.

3.1.1.2.2. 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"

3.1.1.3. 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

3.1.1.4. 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 Organización

3.1.2. 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.

3.1.2.1. 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.

3.1.3. 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.

3.1.4. 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.

3.1.5. 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).

3.1.6. 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.

3.2. 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.

3.2.1. 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.

3.2.2. 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.

3.2.3. 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.

3.2.3.1. 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.

3.2.3.2. 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.

3.2.3.3. 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.

3.2.4. Información de suscriptor no verificada

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

3.2.5. 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.

3.3. Identificación y autenticación de solicitudes de renovación

3.3.1. 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 a las formas y métodos previstos en esta Declaración de Prácticas de Certificación.

3.3.2. 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.

3.4. 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.

4. 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.

4.1. Solicitud de emisión de certificado

4.1.1. 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 .

4.1.2. 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.

4.2. Procesamiento de la solicitud de certificación

4.2.1. 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 .

4.2.2. 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.

4.2.3. 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.

4.3. Emisión del certificado

4.3.1. Acciones de la EC durante el proceso de emisión

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:

- Se protege la confidencialidad e integridad de los datos de registro de que dispone.
- Se utilizan 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.

- Se generan el par de claves, mediante un procedimiento de generación de certificados vinculado de forma segura con el procedimiento de generación de claves.
- Se 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 Bit4id o sus Entidades de Registro deducirlas o utilizarlas en ningún modo.

4.3.2. Notificación de la emisión al suscriptor

Bit4id notifica la emisión del certificado al suscriptor y/o a la persona física identificada en el certificado y el método de generación/descarga.

4.4. Entrega y aceptación del certificado

4.4.1. 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.

4.4.2. 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.

4.4.3. 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 .

4.5. Uso del par de claves y del certificado

4.5.1. Uso por el firmante

El firmante se obliga a:

- Facilitar a la Entidad de Registro información completa y adecuada, conforme a los requisitos de esta 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 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.

4.5.2. Uso por el subscriptor

4.5.2.1. 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 esta 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 esta 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.

4.5.2.2. 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.

4.5.3. Uso por el tercero que confía en certificados

4.5.3.1. 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.

4.5.3.2. 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.

4.6. Renovación de certificados

La renovación de los certificados exige la renovación de claves, por lo que debe atenderse a lo establecido en la sección 4.7.

4.7. Renovación de claves

4.7.1. 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, disponible en la siguiente página web https://web.uanataca.com/pe .

4.7.2. 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, disponible en la siguiente página web https://web.uanataca.com/pe. Los procedimientos de la Entidad de

Registro se realizarán dentro de los límites de esta Declaración de Prácticas de Certificación.

4.7.3. 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, disponible en la siguiente página web https://web.uanataca.com/pe .

4.8. 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.

4.9. 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.

4.9.1. 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 esta 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 del mismo.
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.

4.9.2. 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.

4.9.3. 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.

4.9.4. 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.

4.9.5. 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, disponible 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 de UANATACA. 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 siguiente dirección web:: https://web.uanataca.com/pe.

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

4.9.6. 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.

4.9.7. 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.

4.9.8. 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 Bit4id.

Las Listas de Revocación de Certificados se publican en el repositorio disponible en la siguiente página 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/

4.9.9. 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.

4.9.10. 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.

4.9.11. 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 UANATACA, 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.

4.9.12. 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.

4.9.13. 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.

4.9.14. Período máximo de un certificado digital en estado suspendido

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

4.10. 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 esta Declaración de Prácticas de Certificación. Bit4id puede emitir de oficio un nuevo certificado, mientras los suscriptores mantengan dicho estado.

4.11. Depósito y recuperación de claves

4.11.1. Política y prácticas de depósito y recuperación de claves

Bit4id no presta servicios de depósito y recuperación de claves.

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

Sin estipulación.

5. Controles de seguridad física, de gestión y de operaciones

5.1. Controles de seguridad física

Bit4id a través de la infraestructura de llave pública de UANATACA, S.A. presta sus servicios de certificación, la cual ha establecido controles de seguridad física y ambiental para proteger los recursos de las instalaciones donde se encuentran los sistemas, los propios sistemas y los equipamientos empleados para las operaciones para la prestación de los servicios electrónicos de confianza.

En concreto, la política de seguridad aplicable a los servicios de certificación digital establece prescripciones sobre lo siguiente:

- Controles de acceso físico.
- Protección frente a desastres naturales.
- Medidas de protección frente a incendios.
- Fallo de los sistemas de apoyo (energía electrónica, telecomunicaciones, etc.)
- Derrumbamiento de la estructura.
- Inundaciones.
- Protección antirrobo.
- Salida no autorizada de equipamientos, informaciones, soportes y aplicaciones relativos a componentes empleados para los servicios del prestador de servicios de certificación.

Estas medidas resultan aplicables a las instalaciones desde donde se prestan los servicios de certificación digital, en sus entornos de producción y contingencia, las cuales son auditadas periódicamente de acuerdo con la normativa aplicable y a las políticas propias de UANATACA, S.A. destinadas a este fin.

Las instalaciones cuentan con sistemas de mantenimiento preventivo y correctivo con asistencia 24h-365 días al año con asistencia en las 24 horas siguientes al aviso.

5.1.1. Localización y construcción de las instalaciones

La protección física se logra mediante la creación de perímetros de seguridad claramente definidos en torno a los servicios. La calidad y solidez de los materiales de construcción de las instalaciones garantiza unos adecuados niveles de protección frente a intrusiones por la fuerza bruta y ubicada en una zona de bajo riesgo de desastres y permite un rápido acceso.

La sala donde se realizan las operaciones criptográficas en el Centro de Proceso de Datos cuenta con redundancia en sus infraestructuras, así como varias fuentes alternativas de electricidad y refrigeración en caso de emergencia.

Se dispone de instalaciones que protegen físicamente la prestación de los servicios de aprobación de solicitudes de certificados y de gestión de revocación, del compromiso causado por acceso no autorizado a los sistemas o a los datos, así como a la divulgación de los mismos.

5.1.2. Acceso físico

Se dispone de tres niveles de seguridad física (Entrada del Edificio donde se ubica el CPD, acceso a la sala del CPD y acceso al Rack) para la protección del servicio de generación de certificados, debiendo accederse desde los niveles inferiores a los niveles superiores.

El acceso físico a las dependencias donde se llevan a cabo procesos de certificación está limitado y protegido mediante una combinación de medidas físicas y procedimentales. Así:

- Está limitado a personal expresamente autorizado, con identificación en el momento del acceso y registro del mismo,

incluyendo filmación por circuito cerrado de televisión y su archivo.

- El acceso a las salas se realiza con lectores de tarjeta de identificación y gestionado por un sistema informático que mantiene un log de entradas y salidas automático.
- Para el acceso al rack donde se ubican los procesos criptográficos es necesario la autorización previa de UANATACA a los administradores del servicio de hospedaje que disponen de la llave para abrir la jaula.

5.1.3. Electricidad y aire acondicionado

Las instalaciones disponen de equipos estabilizadores de corriente y un sistema de alimentación eléctrica de equipos duplicado con un grupo electrógeno.

Las salas que albergan equipos informáticos cuentan con sistemas de control de temperatura con equipos de aire acondicionado.

5.1.4. Exposición al agua

Las instalaciones están ubicadas en una zona de bajo riesgo de inundación.

Las salas donde se albergan equipos informáticos disponen de un sistema de detección de humedad.

5.1.5. Prevención y protección de incendios

Las instalaciones y activos de cuentan con sistemas automáticos de detección y extinción de incendios.

5.1.6. Almacenamiento de soportes

Únicamente personal autorizado tiene acceso a los medios de almacenamiento.

La información de más alto nivel de clasificación se guarda en una caja de seguridad fuera de las instalaciones del Centro de Proceso de Datos.

5.1.7. Tratamiento de residuos

La eliminación de soportes, tanto papel como magnéticos, se realizan mediante mecanismos que garantizan la imposibilidad de recuperación de la información.

En el caso de soportes magnéticos, se desechan en cuyo caso se destruyen físicamente, o se reutilizan previo proceso de borrado permanente o formateo. En el caso de documentación en papel, mediante trituradoras o en papeleras dispuestas al efecto para posteriormente ser destruidos, bajo control.

5.1.8. Copia de respaldo fuera de las instalaciones

Se utiliza un almacén externo seguro para la custodia de documentos, dispositivos magnéticos y electrónicos que son independientes del centro de operaciones.

5.2. Controles de procedimientos

Se garantiza que los sistemas de la infraestructura tecnológica se operan de forma segura, para lo cual cuenta con procedimientos para las funciones que afectan a la provisión de sus servicios.

El personal encargado de la prestación del servicio ejecuta los procedimientos administrativos y de gestión de acuerdo con la política de seguridad.

5.2.1. Funciones fiables

Para la prestación de los servicios y administración de la infraestructura se han identificado, las siguientes funciones o roles con la condición de fiables:

- **Auditor Interno:** Responsable del cumplimiento de los procedimientos operativos. Se trata de una persona externa al departamento de Sistemas de Información. Las tareas de Auditor interno son incompatibles en el tiempo con las tareas de Certificación e incompatibles con Sistemas. Estas funciones estarán subordinadas a la jefatura de operaciones, reportando tanto a ésta como a la dirección técnica.
- **Administrador de Sistemas**: Responsable del funcionamiento correcto del hardware y software soporte de la plataforma de certificación
- **Administrador de CA**: Responsable de las acciones a ejecutar con el material criptográfico, o con la realización de alguna función que implique la activación de las claves privadas de las autoridades de certificación descritas en este documento, o de cualquiera de sus elementos.
- **Operador de CA:** Responsable necesario conjuntamente con el Administrador de CA de la custodia de material de activación de las claves criptográficas, también responsable de las operaciones de copia de respaldo y mantenimiento de la AC.
- **Operador de Registro:** Persona responsable de aprobar las peticiones de certificación realizadas por el suscriptor y emitir certificados digitales.
- **Responsable de Seguridad**: Encargado de coordinar, controlar y hacer cumplir las medidas de seguridad definidas por las políticas de seguridad. Debe encargarse de los aspectos

relacionados con la seguridad de la información: lógica, física, redes, organizativa, etc.

Las personas que ocupan los puestos anteriores se encuentran sometidas a procedimientos de investigación y control específicos. Adicionalmente, se han implementado criterios en sus políticas para la segregación de las funciones, como medida de prevención de actividades fraudulentas.

5.2.2. Número de personas por tarea

A la hora de llevar a cabo la prestación del servicio se garantiza al menos dos personas para realizar las tareas relativas a la generación, recuperación y back-up de la clave privada de las Autoridades de Certificación. Igual criterio se aplica para la ejecución de tareas de emisión y activación de certificados y claves privadas de las Autoridades de Certificación, y en general cualquier manipulación del dispositivo de custodia de las claves de la Autoridad de Certificación raíz e intermedias.

5.2.3. Identificación y autenticación para cada función

Las personas asignadas para cada rol son identificadas por el auditor interno que se asegurará que cada persona realiza las operaciones para las que está asignado.

Cada persona solo controla los activos necesarios para su rol, asegurando así que ninguna persona accede a recursos no asignados.

El acceso a recursos se realiza dependiendo del activo mediante usuario/contraseña, certificado digital, tarjeta de acceso físico y/o llaves.

5.2.4. Roles que requieren separación de tareas

Las siguientes tareas son realizadas, al menos, por dos personas:

- Las tareas propias del rol de Auditor serán incompatibles con la operación y administración de sistemas, y en general aquellas

dedicadas a la prestación directa de los servicios electrónicos de confianza.

- Emisión y revocación de certificados, serán tareas incompatibles con la Administración y operación de los sistemas.
- La administración y operación de los sistemas y las CAs, serán incompatibles entre sí.

5.2.5. Sistema de gestión PKI

El sistema de PKI se compone de los siguientes módulos:

- Componente/módulo de gestión de las Autoridades de Certificación Subordinadas.
- Componente/módulo de gestión de la Autoridad de Registro.
- Componente/módulo de gestión de solicitudes.
- Componente/módulo de gestión de claves (HSM).
- Componente/módulo de bases de datos.
- Componente/módulo de gestión de CRL.
- Componente/módulo de gestión de la Autoridad de Validación (servicios de OCSP).

5.3. Controles de personal

5.3.1. Requisitos de historial, calificaciones, experiencia y autorización

Todo el personal está cualificado y/o ha sido instruido convenientemente para realizar las operaciones que le han sido asignadas.

El personal en puestos de confianza no tiene intereses personales que entran en conflicto con el desarrollo de la función que tenga encomendada.

En general, se retirará de sus funciones de confianza a una persona, cuando se tenga conocimiento de la existencia de conflictos de interés y/o la comisión de algún hecho delictivo que pudiera afectar al desempeño de sus funciones.

No se asignará a un sitio confiable o de gestión a una persona que no sea idónea para el puesto, especialmente por una falta que afecte su capacidad para el mismo. Por este motivo, previamente se realiza una investigación en el marco de la legislación aplicable, relativa a los siguientes aspectos:

- Estudios, incluyendo titulación alegada.
- Trabajos anteriores, hasta cinco años, incluyendo referencias profesionales.
- Referencias profesionales.

5.3.2. Procedimientos de investigación de historial

Con carácter previo a la asignación de una persona o de que ésta acceda al puesto de trabajo, se realizan las siguientes comprobaciones:

- Referencias de los trabajos de los últimos años.
- Referencias profesionales.
- Estudios, incluyendo titulación alegada.

Dicha investigación se realiza siempre previo consentimiento inequívoco del afectado, y se procesa y protege todos sus datos personales de acuerdo con la normativa de Protección de Datos aplicable a cada caso.

Todas las comprobaciones se realizan hasta donde lo permite la legislación vigente aplicable. Los motivos que pueden dar lugar a rechazar al candidato a un puesto fiable son los siguientes:

- Falsedades en la solicitud de trabajo, realizadas por el candidato.
- Referencias profesionales muy negativas o muy poco fiables en relación con el candidato.

5.3.3. Requisitos de formación

El personal que ocupa puestos fiables y de gestión, recibe formación hasta que alcanzan la cualificación necesaria para el desempeño de sus funciones, manteniendo archivo de dicha formación.

Los programas de formación son revisados periódicamente, y son actualizados y mejorados de forma periódica.

La formación incluye, al menos, los siguientes contenidos:

- Principios y mecanismos de seguridad de la jerarquía de certificación, así como el entorno de usuario de la persona a formar.
- Tareas que debe realizar la persona.
- Políticas y procedimientos de seguridad correspondientes. Uso y operación de maquinaria y aplicaciones instaladas.
- Gestión y tramitación de incidentes y compromisos de seguridad.
- Procedimientos de continuidad de negocio y emergencia.
- Procedimiento de gestión y de seguridad en relación con el tratamiento de los datos de carácter personal.

5.3.4. Requisitos y frecuencia de actualización formativa

La formación del personal se actualiza de acuerdo con las necesidades, y con la frecuencia suficiente para cumplir sus funciones de forma competente y satisfactoria, especialmente cuando se realicen modificaciones sustanciales en las tareas de certificación.

5.3.5. Secuencia y frecuencia de rotación laboral

No aplicable.

5.3.6. Sanciones para acciones no autorizadas

Se dispone de un sistema sancionador, para depurar las responsabilidades derivadas de acciones no autorizadas, adecuado a la legislación laboral aplicable.

Las acciones disciplinarias incluyen la suspensión, separación de las funciones y hasta el despido de la persona responsable de la acción dañina, de forma proporcionada a la gravedad de la acción no autorizada.

5.3.7. Requisitos de contratación de profesionales

Los empleados contratados para realizar tareas confiables firman con anterioridad las cláusulas de confidencialidad y los requerimientos operacionales empleados para llevar a cabo la prestación de servicios de certificación correspondientes. Cualquier acción que comprometa la seguridad de los procesos aceptados podría, una vez evaluados, dar lugar al cese de la designación para el rol fiable.

En el caso de que todos o parte de los servicios de certificación sean operados por un tercero, los controles y previsiones realizadas en esta sección, o en otras partes de la Declaración de Prácticas de Certificación, serán aplicados y cumplidos por el tercero que realice las funciones de operación de los servicios de certificación, no obstante, la entidad de certificación será responsable en todo caso de la efectiva ejecución. Estos aspectos quedan concretados en el instrumento jurídico utilizado para acordar la prestación de los servicios de certificación por un tercero.

5.3.8. Suministro de documentación al personal

Todo el personal recibirá la documentación que estrictamente precise en cada momento, al objeto de realizar su trabajo de forma competente y satisfactoria.

5.4. Procedimientos de auditoría de seguridad

5.4.1. Tipos de eventos registrados

Se producen y guardan registro, al menos, de los siguientes eventos relacionados con la seguridad de la entidad:

- Encendido y apagado del sistema.
- Intentos de creación, borrado, establecimiento de contraseñas o cambio de privilegios.
- Intentos de inicio y fin de sesión.
- Intentos de accesos no autorizados al sistema de la AC a través de la red.
- Intentos de accesos no autorizados al sistema de archivos.
- Acceso físico a los logs.
- Cambios en la configuración y mantenimiento del sistema.
- Registros de las aplicaciones de la AC.
- Encendido y apagado de la aplicación de la AC.
- Cambios en los detalles de la AC y/o sus claves.
- Cambios en la creación de políticas de certificados.
- Generación de claves propias.
- Creación y revocación de certificados.
- Registros de la destrucción de los medios que contienen las claves, datos de activación.
- Eventos relacionados con el ciclo de vida del módulo criptográfico, como recepción, uso y desinstalación de éste.
- La ceremonia de generación de claves y las bases de datos de gestión de claves.
- Registros de acceso físico.
- Mantenimientos y cambios de configuración del sistema.
- Cambios en el personal.
- Informes de compromisos y discrepancias.
- Registros de la destrucción de material que contenga información de claves, datos de activación o información personal del suscriptor, en caso de certificados individuales, o

de la persona natural identificada en el certificado, en caso de certificados de organización.
- Posesión de datos de activación, para operaciones con la clave privada de la Entidad de Certificación.
- Informes completos de los intentos de intrusión física en las infraestructuras que dan soporte a la emisión y gestión de certificados.

Las entradas del registro incluyen los siguientes elementos:
- Fecha y hora de la entrada.
- Número de serie o secuencia de la entrada, en los registros automáticos.
- Identidad de la entidad que entra el registro.
- Tipo de entrada.

5.4.2. Frecuencia de tratamiento de registros de auditoría

Se revisan los logs cuando se produce una alerta del sistema motivada por la existencia de algún incidente.

El procesamiento de los registros de auditoría consiste en una revisión de los registros que incluye la verificación de que éstos no han sido manipulados, una breve inspección de todas las entradas de registro y una investigación más profunda de cualquier alerta o irregularidad en los registros. Las acciones realizadas a partir de la revisión de auditoría están documentadas.

Se mantiene un sistema que permite garantizar:
- Espacio suficiente para el almacenamiento de logs.
- Que los ficheros de logs no se reescriben.
- Que la información que se guarda incluye como mínimo: tipo de evento, fecha y hora, usuario que ejecuta el evento y resultado de la operación.
- Los ficheros de logs se guardarán en ficheros estructurados susceptibles de incorporar en una BBDD para su posterior exploración.

5.4.3. Período de conservación de registros de auditoría

Se almacena la información de los logs durante un periodo de entre 1 y 15 años, en función del tipo de información registrada.

5.4.4. Protección de los registros de auditoría

Los logs de los sistemas:

- Están protegidos de manipulación mediante la firma de los ficheros que los contienen.
- Son almacenados en dispositivos ignífugos.
- Se protege su disponibilidad mediante su almacenamiento en instalaciones externas al centro donde se ubica la EC.

El acceso a los ficheros de logs está reservado solo a las personas autorizadas. Asimismo, los dispositivos son manejados en todo momento por personal autorizado.

Existe un procedimiento interno donde se detallan los procesos de gestión de los dispositivos que contienen datos de logs de auditoría.

5.4.5. Procedimientos de copia de respaldo

Se dispone de un procedimiento adecuado de backup de manera que, en caso de pérdida o destrucción de archivos relevantes, estén disponibles en un periodo corto de tiempo las correspondientes copias de backup de los logs.

Se tiene implementado un procedimiento de backup seguro de los logs de auditoría, realizando semanalmente una copia de todos los logs en un medio externo. Adicionalmente se mantiene copia en centro de custodia externo.

5.4.6. Localización del sistema de acumulación de registros de auditoría

La información de la auditoria de eventos es recogida internamente y de forma automatizada por el sistema operativo, las comunicaciones de red y por el software de gestión de certificados, además de por los datos manualmente generados, que serán almacenados por el personal debidamente autorizado. Todo ello compone el sistema de acumulación de registros de auditoría.

5.4.7. Notificación del evento de auditoría al causante del evento

Cuando el sistema de acumulación de registros de auditoría registre un evento, no es preciso enviar una notificación al individuo, organización, dispositivo o aplicación que causó el evento.

5.4.8. Análisis de vulnerabilidades

El análisis de vulnerabilidades queda cubierto por los procesos de auditoría.

Los análisis de vulnerabilidad deben ser ejecutados, repasadas y revisadas por medio de un examen de estos acontecimientos monitorizados. Estos análisis deben ser ejecutados periódicamente de acuerdo con el procedimiento interno que previsto para este fin.

Los datos de auditoría de los sistemas son almacenados con el fin de ser utilizados en la investigación de cualquier incidencia y localizar vulnerabilidades.

5.5. Archivos de informaciones

Se garantiza que toda la información relativa a los certificados se conserva durante un período de tiempo apropiado, según lo establecido en este documento.

5.5.1. Tipos de registros archivados

De acuerdo con la normativa aplicable los siguientes documentos implicados en el ciclo de vida del certificado son almacenados por la Entidad de Certificación o bien por la Entidad de Registro:

- Todos los datos de auditoría de sistema.
- Todos los datos relativos a los certificados, incluyendo los contratos con los firmantes y los datos relativos a su identificación y su ubicación
- Solicitudes de emisión y revocación de certificados.
- Tipo de documento presentado en la solicitud del certificado.
- Identidad de la Entidad de Registro que acepta la solicitud de certificado.
- Número de identificación único proporcionado por el documento anterior.
- Todos los certificados emitidos o publicados.
- CRLs emitidas o registros del estado de los certificados generados.
- El historial de claves generadas.
- Las comunicaciones entre los elementos de la PKI.
- Políticas y Prácticas de Certificación
- Todos los datos de auditoría identificados en la sección 5.4
- Información de solicitudes de certificación.
- Documentación aportada para justificar las solicitudes de certificación.
- Información del ciclo de vida del certificado.

Bit4id y las Entidades de Registro cuando corresponda, serán responsables del correcto archivo de todo este material.

5.5.2. Período de conservación de registros

Los registros especificados anteriormente se archivan durante al menos 15 años, o el período que establezca la legislación vigente.

En particular, los registros de certificados revocados estarán accesibles para su libre consulta durante al menos 15 años o el periodo que establezca la legislación vigente desde su cambio de estado.

5.5.3. Protección del archivo

El archivo se protege de forma que sólo personas debidamente autorizadas puedan obtener acceso al mismo. El archivo es protegido contra visualización, modificación, borrado o cualquier otra manipulación mediante su almacenamiento en un sistema fiable.

Asimismo se asegura la correcta protección de los archivos mediante la asignación de personal cualificado para su tratamiento y el almacenamiento en instalaciones seguras externas.

5.5.4. Procedimientos de copia de respaldo

Se dispone de un centro de almacenamiento externo para garantizar la disponibilidad de las copias del archivo de ficheros electrónicos. Los documentos físicos se encuentran almacenados en lugares seguros de acceso restringido solo a personal autorizado.

Como mínimo se realizan copias de respaldo incrementales diarias de todos sus documentos electrónicos y copias de respaldo completas semanalmente para casos de recuperación de datos.

Además, guarda copia de los documentos en papel en un lugar seguro diferente de las instalaciones de la propia Entidad de certificación.

5.5.5. Requisitos de sellado de fecha y hora

Los registros están fechados con una fuente fiable vía NTP.

No es necesario que esta información se encuentre firmada digitalmente.

5.5.6. Localización del sistema de archivo

Se dispone de un sistema centralizado de recogida de información de la actividad de los equipos implicados en el servicio de gestión de certificados.

5.5.7. Procedimientos de obtención y verificación de información de archivo

Se dispone de un procedimiento donde se describe el proceso para verificar que la información archivada es correcta y accesible. Asimismo proporciona la información y medios de verificación al auditor.

5.6. Renovación de claves

Con anterioridad a que el uso de la clave privada de la AC caduque, será realizado un cambio de claves. La antigua AC y su clave privada solo se usarán para la firma de CRLs mientras existan certificados activos emitidos por dicha AC. Se generará una nueva AC con una clave privada nueva y un nuevo DN. El cambio de claves del suscriptor es realizado mediante la realización de un nuevo proceso de emisión.

Alternativamente, en el caso de Autoridades de Certificación subordinadas, se podrá optar por la renovación del certificado con o sin cambio de claves, no resultando aplicable el procedimiento antes descrito.

5.7. Compromiso de claves y recuperación de desastre

5.7.1. Procedimientos de gestión de incidencias y compromisos

Se prevé políticas de seguridad y continuidad del negocio que le permiten la gestión y recuperación de los sistemas en caso de incidentes y compromiso de sus operaciones, asegurando los servicios críticos de revocación y publicación del estado de los certificados.

5.7.2. Corrupción de recursos, aplicaciones o datos

Cuando acontezca un evento de corrupción de recursos, aplicaciones o datos, se seguirán los procedimientos de gestión oportunos de acuerdo con las políticas de seguridad y gestión de incidentes de Bit4id, que contemplan escalado, investigación y respuesta al incidente. Si resulta necesario, se iniciarán los procedimientos de compromiso de claves o de recuperación de desastres de Bit4id.

5.7.3. Compromiso de la clave privada de la entidad

En caso de sospecha o conocimiento del compromiso, se activarán los procedimientos de compromiso de claves de acuerdo con las políticas de seguridad, gestión de incidencias y continuidad del negocio, que permita la recuperación de los sistemas críticos, si fuera necesario en un centro de datos alternativo.

5.7.4. Continuidad del negocio después de un desastre

Se restablecerán los servicios críticos (suspensión y revocación, y publicación de información de estado de certificados) de acuerdo con el plan de incidencias y continuidad de negocio existente restaurando la operación normal de los servicios anteriores en las 24 horas siguientes al desastre.

Se dispone de un centro alternativo en caso de ser necesario para la puesta en funcionamiento de los sistemas de certificación descritos en el plan de continuidad de negocio.

5.8. Terminación del servicio

5.8.1. Cese de Bit4id

Se asegura que las posibles interrupciones a los suscriptores y a terceras partes son mínimas como consecuencia del cese de los servicios del prestador de servicios de certificación digital. En este sentido, Se garantiza un mantenimiento continuo de los registros definidos en esta Declaración de Prácticas de Certificación.

No obstante lo anterior, si procede se ejecutarán todas las acciones que sean necesarias para transferir a un tercero o a un depósito notarial, las obligaciones de mantenimiento de los registros especificados durante el periodo correspondiente según esta Declaración de Prácticas de Certificación o la previsión legal que corresponda.

Antes de terminar sus servicios, se desarrolla un plan de terminación, con las siguientes provisiones:

- Proveerá de los fondos necesarios, incluyendo un seguro de responsabilidad civil, para continuar la finalización de las actividades de revocación.
- Informará a todos Firmantes/Suscriptores, Tercero que confían y otras EC's con los cuales tenga acuerdos u otro tipo de relación del cese con una anticipación mínima de 6 meses.
- Revocará toda autorización a entidades subcontratadas para actuar en nombre de la EC en el procedimiento de emisión de certificados.
- Transferirá sus obligaciones relativas al mantenimiento de la información del registro y de los logs durante el periodo de tiempo indicado a los suscriptores y usuarios.
- Destruirá o deshabilitará para su uso las claves privadas de la EC.
- Mantendrá los certificados activos y el sistema de verificación y revocación hasta la extinción de todos los certificados emitidos.

- Ejecutará las tareas necesarias para transferir las obligaciones de mantenimiento de la información de registro y los archivos de registro de eventos durante los períodos de tiempo respectivos indicados al suscriptor y a los terceros que confían en certificados.

5.8.2. Comunicación del cese

Antes de la finalización de sus servicios como Entidad de Certificación y con una antelación de treinta (30) días, comunicará el cese a INDECOPI, a los suscriptores, titulares y terceros que puedan verse afectados con el cese de sus operaciones.

Sin perjuicio de las comunicaciones especificadas en el presente apartado,se publicará el detalle de la finalización de los servicios y del cese efectivo en la siguiente dirección: https://web.uanataca.com/pe.

Con respecto de los procedimientos a ejecutar con respecto del cese:

- Procederá a la terminación de las autorizaciones de todos los subcontratistas y en general de cualquier tercero que actúe en nombre de Bit4id o participe en el proceso de emisión de certificados digitales.
- Todas las solicitudes y contratos de suscriptores, así como los archivos de log de eventos y registros de auditorías, se remitirán a INDECOPI o bien, cuando así lo haya determinado este último, se transferirán a otra Entidad de Certificación debidamente autorizada. Asimismo, también se transferirán los certificados de la Autoridad de Certificación raíz y las listas de certificados revocados (CRL).
- Mantendrá disponible la clave pública de la Autoridad de Certificación durante un periodo razonable de tiempo.
- Se deshabilitarán las claves privadas así como las copias de respaldo de tal manera que sea imposible su recuperación o utilización para la prestación de este servicio.

6. Controles de seguridad técnica

Se emplean sistemas y productos fiables, protegidos contra toda alteración y que garantizan la seguridad técnica y criptográfica de los procesos de certificación a los que sirven de soporte.

6.1. Generación e instalación del par de claves

6.1.1. 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.

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

6.1.1.1. 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.

6.1.2. 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.

6.1.3. 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.

6.1.4. 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.

6.1.5. 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.

6.1.6. 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.

6.1.7. Comprobación de calidad de parámetros de clave pública

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

6.1.8. 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.

6.1.9. 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, el no repudio y cifrado de datos.

6.2. Protección de la clave privada

6.2.1. 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.

6.2.2. 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 esta 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.

6.2.3. Depósito de la clave privada

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

6.2.4. 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.

6.2.5. 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.

6.2.6. Introducción de la clave privada en el módulo criptográfico

Las claves privadas se generan directamente en los módulos criptográficos.

6.2.7. Método de activación de la clave privada

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

6.2.8. 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 6.2.2.

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.

6.2.9. 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.

6.2.10. 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.

6.2.11. Clasificación de módulos criptográficos

Ver la sección 6.2.1.

6.3. Otros aspectos de gestión del par de claves

6.3.1. Archivo de la clave pública

Se archivan sus claves públicas de forma rutinaria, de acuerdo con lo establecido en la sección 5.5 de este documento.

6.3.2. 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.

6.4. Datos de activación

6.4.1. Generación e instalación de datos de activación

Los datos de activación de los dispositivos que protegen las claves privadas son generados de acuerdo con lo establecido en la sección 6.2.2 y los procedimientos de ceremonia de claves.

La creación y distribución de dichos dispositivos es registrada.

Asimismo, se generan de forma segura los datos de activación.

6.4.2. Protección de datos de activación

Los datos de activación de los dispositivos que protegen las claves privadas de las Autoridades de certificación raíz y subordinadas, están protegidos por los poseedores de las tarjetas de administradores de los módulos criptográficos, según consta en el documento de ceremonia de claves.

El firmante del certificado es el responsable de la protección de su clave privada, con una o varias contraseñas lo más completas y complejas posible. El firmante debe recordar dicha(s) contraseña(s).

6.5. Controles de seguridad informática

Se emplea sistemas fiables para ofrecer sus servicios de certificación. La Entidad de Certificación ha realizado controles y auditorias informáticas a fin de establecer una gestión de sus activos informáticos adecuados con el nivel de seguridad requerido en la gestión de sistemas de certificación electrónica.

Respecto a la seguridad de la información se aplican controles del esquema de certificación sobre sistemas de gestión de la información ISO 27001.

Los equipos usados son inicialmente configurados con los perfiles de seguridad adecuados por parte del personal de sistemas, en los siguientes aspectos:

- Configuración de seguridad del sistema operativo.
- Configuración de seguridad de las aplicaciones.
- Dimensionamiento correcto del sistema.
- Configuración de Usuarios y permisos.
- Configuración de eventos de Log.
- Plan de backup y recuperación.
- Configuración antivirus.
- Requerimientos de tráfico de red.

6.5.1. Requisitos técnicos específicos de seguridad informática

Cada servidor incluye las siguientes funcionalidades:

- Control de acceso a los servicios de las Autoridades de Certificación subordinadas y gestión de privilegios.
- Imposición de separación de tareas para la gestión de privilegios.
- Identificación y autenticación de roles asociados a identidades.
- Archivo del historial del suscriptor, de las Autoridades de Certificación subordinadas y datos de auditoria.
- Auditoria de eventos relativos a la seguridad.
- Auto-diagnóstico de seguridad relacionado con los servicios de las Autoridades de Certificación subordinadas.
- Mecanismos de recuperación de claves y del sistema de las Autoridades de Certificación subordinadas.

Las funcionalidades expuestas son realizadas mediante una combinación de sistema operativo, software de PKI, protección física y procedimientos.

6.5.2. Evaluación del nivel de seguridad informática

Las aplicaciones de autoridad de certificación y de registro empleadas son fiables.

6.6. Controles técnicos del ciclo de vida

6.6.1. Controles de desarrollo de sistemas

Las aplicaciones son desarrolladas e implementadas por de acuerdo con estándares de desarrollo y control de cambios.

Las aplicaciones disponen de métodos para la verificación de la integridad y autenticidad, así como de la corrección de la versión a emplear.

6.6.2. Controles de gestión de seguridad

Se desarrollan las actividades precisas para la formación y concienciación en materia de seguridad de las personas encargadas de prestar los servicios de certificación. Los materiales empleados para la formación y los documentos descriptivos de los procesos, son actualizados después de su aprobación por un grupo para la gestión de la seguridad. En la realización de esta función dispone de un plan de formación anual.

Se exige mediante contrato, las medidas de seguridad equivalentes a cualquier proveedor externo implicado en las labores de servicios electrónicos de confianza.

6.6.2.1. Clasificación y gestión de información y bienes

Se mantiene un inventario de activos y documentación y un procedimiento para la gestión de este material para garantizar su uso.

La política de seguridad de información detalla los procedimientos de gestión de la información donde se clasifica según su nivel de confidencialidad.

Los documentos están catalogados en tres niveles: SIN CLASIFICAR, USO INTERNO y CONFIDENCIAL.

6.6.2.2. Operaciones de gestión

Se dispone de un adecuado procedimiento de gestión y respuesta de incidencias, mediante la implementación de un sistema de alertas y la generación de reportes periódicos.

En el documento de seguridad de se desarrolla en detalle el proceso de gestión de incidencias.

Se tiene documentado todo el procedimiento relativo a las funciones y responsabilidades del personal implicado en el control y manipulación de elementos contenidos en el proceso de certificación.

6.6.2.3. Tratamiento de los soportes y seguridad

Todos los soportes son tratados de forma segura de acuerdo con los requisitos de la clasificación de la información. Los soportes que contengan datos sensibles son destruidos de manera segura si no van a volver a ser requeridos.

Planificación del sistema

Se mantiene un registro de las capacidades de los equipos. Conjuntamente con la aplicación de control de recursos de cada sistema se puede prever un posible redimensionamiento.

Reportes de incidencias y respuesta

Se dispone de un procedimiento para el seguimiento de incidencias y su resolución donde se registran las respuestas y una evaluación económica que supone la resolución de la incidencia.

Procedimientos operacionales y responsabilidades

Se definen actividades, asignadas a personas con un rol de confianza, distintas de las personas encargadas de realizar las operaciones cotidianas que no tienen carácter de confidencialidad.

6.6.2.4. Gestión del sistema de acceso

Se realizan todos los esfuerzos que razonablemente están a su alcance para confirmar que el sistema de acceso está limitado a las personas autorizadas.

En particular:

AC General

- Se dispone de controles basados en firewalls, antivirus e IDS en alta disponibilidad.
- Los datos sensibles son protegidos mediante técnicas criptográficas o controles de acceso con identificación fuerte.
- Se dispone de un procedimiento documentado de gestión de altas y bajas de usuarios y política de acceso detallado en su política de seguridad.
- Se dispone de procedimientos para asegurar que las operaciones se realizan respetando la política de roles.
- Cada persona tiene asociado un rol para realizar las operaciones de certificación.
- El personal es responsable de sus actos mediante el compromiso de confidencialidad firmado con la empresa.

Generación del certificado

La autenticación para el proceso de emisión se realiza mediante un sistema m de n operadores para la activación de la clave privada.

Gestión de la revocación

La revocación se realizará mediante autenticación fuerte a las aplicaciones de un administrador autorizado. Los sistemas de logs generarán las pruebas que garantizan el no repudio de la acción realizada por el administrador.

Estado de la revocación

La aplicación del estado de la revocación dispone de un control de acceso basado en la autenticación con certificados o con doble factor de identificación para evitar el intento de modificación de la información del estado de la revocación.

6.6.2.5. Gestión del ciclo de vida del hardware criptográfico

Se toman medidas para asegurar que el hardware criptográfico usado para la firma de certificados no se manipula durante su transporte mediante la inspección del material entregado.

El hardware criptográfico se traslada sobre soportes preparados para evitar cualquier manipulación.

Se registra toda la información pertinente del dispositivo para añadir al catálogo de activos.

El uso del hardware criptográfico de firma de certificados requiere el uso de al menos dos empleados de confianza.

Se realiza test de pruebas periódicas para asegurar el correcto funcionamiento del dispositivo.

El dispositivo hardware criptográfico solo es manipulado por personal confiable.

La clave privada de firma se almacenada en el hardware criptográfico se eliminará una vez se ha retirado el dispositivo.

La configuración del sistema así como sus modificaciones y actualizaciones son documentadas y controladas.

Los cambios o actualizaciones son autorizados por el responsable de seguridad y quedan reflejados en las actas de trabajo correspondientes. Estas configuraciones se realizarán al menos por dos personas confiables.

6.7. Controles de seguridad de red

Se protege el acceso físico a los dispositivos de gestión de red, y dispone de una arquitectura que ordena el tráfico generado basándose en sus características de seguridad, creando secciones de red claramente definidas. Esta división se realiza mediante el uso de cortafuegos.

La información confidencial que se trasfiere por redes no seguras, se realiza de forma cifrada mediante uso de protocolos SSL o del sistema VPN con autenticación por doble factor.

6.8. Controles de ingeniería de módulos criptográficos

Los módulos criptográficos se someten a los controles de ingeniería previstos en las normas indicadas a lo largo de esta sección.

Los algoritmos de generación de claves empleados se aceptan comúnmente para el uso de la clave a que están destinados.

Todas las operaciones criptográficas se realizan en módulos con las certificaciones FIPS 140-2 nivel 3.

6.9. Fuentes de Tiempo

Se tiene un procedimiento de sincronización de tiempo coordinado vía NTP, que accede a dos servicios independientes:

- La primera sincronización es con un servicio basado en antenas y receptores GPS que permite un nivel de confianza de STRATUM 1 (con dos sistemas en alta disponibilidad).
- La segunda dispone de una sincronización complementaria, vía NTP, con el Real Instituto y Observatorio de la Armada (ROA).

6.10. Cambio de estado de un Dispositivo Seguro de Creación de Firma

En el caso de modificación del estado de la certificación de los dispositivos de creación de firma procederá de la siguiente manera:

a) Se dispone de una lista de varios dispositivos de creación de firma certificados, así como una estrecha relación con proveedores de dichos dispositivos, con el fin de garantizar alternativas a posibles pérdidas de estado de certificación de dispositivos seguros para la creación de firmas.
b) En el supuesto de finalización del periodo de validez o pérdida de la certificación, no utilizará dichos dispositivos para la emisión de nuevos certificados digitales, bien sea en nuevas emisiones como eventualmente en posibles renovaciones.
c) Procederá de inmediato a cambiar a de dispositivos con certificación apropiada.
d) En el supuesto caso que un dispositivo seguro haya demostrado no haberlo sido nunca, por falsificación o cualquier otro tipo de fraude, se procederá de inmediato a comunicárselo a sus clientes y al ente regulador, revocar los certificados digitales emitidos en estos dispositivos y reemplazarlos emitiéndolos en dispositivos seguros de creación de firma.

6.11. Protocolo de comunicación entre la ER y la EC

La Entidad de Registro vinculada, cuando lleve a cabo el registro de las solicitudes de certificados electrónicos, así como cuantas acciones que afecten al ciclo de vida de los certificados, éstas se realizarán mediante conexión a una aplicación web denominada "Autoridad de registro – RA".

Cada operador de la ER vinculada efectúa el acceso a dicha aplicación con certificado electrónico. A la hora de aprobar y/o generar una solicitud (la generación es la operación a través de la cual se emite el certificado electrónico asociado a la solicitud), la aplicación de RA presenta al operador unas evidencias a firmar. Dichas evidencias, una vez firmadas electrónicamente con el certificado del operador, son custodiadas y almacenadas directamente por parte de la aplicación de RA.

A la hora de emitir un certificado, la aplicación de RA genera un CSR (Certificate Signing Request) en formato pkcs#10 que, junto con las evidencias descritas en el párrafo anterior, es enviado al back-end de la Entidad de Certificación.

La Entidad de Certificación devuelve el certificado a la aplicación de RA de manera que sea almacenado en el dispositivo criptográfico/elemento seguro de referencia.

Todos los eventos asociados a la generación del certificado, así como aquellos que afecten al ciclo de vida de los certificados y todos los mensajes intercambiados entre de la aplicación de RA y le back-end de la Entidad de Certificación son debidamente trazados y almacenados de forma segura para efectuar auditorías.

Con este protocolo se garantiza la responsabilidad de cada componente involucrado en la generación y gestión del ciclo de vida de

cada certificado y el no repudio entre de Entidad de Registro vinculada y la Entidad de Certificación.

7. Perfiles de certificados y listas de certificados revocados

7.1. 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.

7.1.1. Número de versión

Bit4id emite certificados X.509 Versión 3.

7.1.2. 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.

7.1.3. 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

7.1.4. Formato de Nombres

Los certificados deberán contener las informaciones que resulten necesarias para su uso, según determine la correspondiente política.
Las restricciones de políticas son establecidas conforme al RFC 3280.

7.1.5. Restricción de los nombres

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

7.1.6. 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.

La sintaxis y la semántica de los calificadores de política son conforme al RFC 3280.

Bit4id soporta cualquiera de las extensiones estandarizadas definidas en el RFC 3280 sea que estas se encuentren marcadas o no como críticas.

Bit4id no marca como criticas las extensiones no estandarizadas en los certificados que pretendan ser usados fuera del ámbito de la IOFE.

Bit4id somete previamente a INDECOPI cualquier cambio que afecte los OID de cualquiera de los certificados y políticas definidos en el presente documento.

Los controles de la versión son utilizados para asegurar que las políticas y prácticas vigentes al momento de archivar una transacción, puedan ser establecidas.

7.2. Perfil de la lista de revocación de certificados

7.2.1. Número de versión

Las CRL emitidas por Bit4id son de la versión 2. Bit4idsoporta extensiones CRL conformes al RFC 5280.

7.2.2. Perfil de OCSP

Según el estándar IETF RFC 6960 y el estándar X.509 versión 3.

8. Auditoría de conformidad

UANATACA S.A., como Proveedor de Servicios de Certificación de BIT4ID SAC, se encuentra sometida a revisiones de control y está sujeto a auditorías de conformidad periódicas para la adecuación al 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), para la evaluación de la conformidad de prestadores cualificados de servicios de confianza, bajo las normas ISO/IEC 17065:2012, ETSI EN 319 403 V2.2.2., y más concretamente con respecto los siguientes servicios certificables:

- Servicio de expedición de sellos electrónicos de tiempo. Especificaciones técnicas utilizadas:
    - ETSI EN 319 421 v1.1.1 Policy and Security Requirements for Trust Service Providers issuing Time-Stamps.
    - ETSI EN 319 401 v2.1.1 General Policy Requirements for Trust Service Providers.

- Servicio de expedición de certificados electrónicos de firma digital. Especificaciones técnicas utilizadas:
    - *ETSI EN 319 411-2 v 2.1.1 Policy and security requirements for Trust Service Providers issuing certificates: Requirements for trust service providers issuing EU qualified certificates.*
    - *ETSI EN 319 411-1 v 1.1.1 Policy and security requirements for Trust Service Providers issuing certificates: General requirements.*
    - *ETSI EN 319 401 v2.1.1 General Policy Requirements for Trust Service Providers.*

- Servicio de expedición de certificados electrónicos de sello digital. Especificaciones técnicas utilizadas:

- *ETSI EN 319 411-2 v 2.1.1 Policy and security requirements for Trust Service Providers issuing certificates: Requirements for trust service providers issuing EU qualified certificates.*
- *ETSI EN 319 411-1 v 1.1.1 Policy and security requirements for Trust Service Providers issuing certificates: General requirements.*
- *ETSI EN 319 401 v2.1.1 General Policy Requirements for Trust Service Providers.*

8.1. Frecuencia de la auditoría de conformidad

Bit4id lleva a cabo una auditoría para la evaluación de su conformidad anualmente, además de las auditorías internas que realiza bajo su propio criterio o en cualquier momento, debido a una sospecha de incumplimiento de alguna medida de seguridad.

8.2. Identificación y calificación del auditor

Las auditorías son realizadas por una firma de auditoría independiente externa que demuestra competencia técnica y experiencia en seguridad informática, en seguridad de sistemas de información y en auditorías de conformidad de servicios de certificación de clave pública, y los elementos relacionados.

8.3. Relación del auditor con la entidad auditada

Las empresas de auditoría son de reconocido prestigio con departamentos especializados en la realización de auditorías informáticas, por lo que no existe ningún conflicto de intereses que pueda desvirtuar su actuación en relación con Bit4id.

8.4. Listado de elementos objeto de auditoría

La auditoría verifica respecto a Bit4id:

a) Que la entidad tiene un sistema de gestión que garantiza la calidad del servicio prestado.
b) Que la entidad cumple con los requerimientos de la Declaración de Prácticas de Certificación y otra documentación vinculada con la emisión de los distintos certificados digitales.
c) Que la Declaración de Prácticas de Certificación y demás documentación jurídica vinculada, se ajusta a lo acordado y con lo establecido en la normativa vigente.
d) Que la entidad gestiona de forma adecuada sus sistemas de información

En particular, los elementos objeto de auditoría serán los siguientes:

a) Procesos de las Autoridades de Certificación y elementos relacionados.
b) Sistemas de información.
c) Protección del centro de proceso de datos.
d) Documentos.

8.5. Acciones a emprender como resultado de una falta de conformidad

Una vez recibido por la dirección el informe de la auditoría de cumplimiento realizada, se analizan, con la firma que ha ejecutado la auditoría, las deficiencias encontradas y desarrolla y ejecuta las medidas correctivas que solventen dichas deficiencias.

Si hubiese incapacidad de desarrollar y/o ejecutar las medidas correctivas o si las deficiencias encontradas suponen una amenaza inmediata para la seguridad o integridad del sistema, deberá comunicarlo inmediatamente al Comité de Seguridad que podrá ejecutar las siguientes acciones:

- Cesar las operaciones transitoriamente.

- Revocar la clave de la Autoridad de Certificación y regenerar la infraestructura.
- Terminar el servicio de la Autoridad de Certificación.
- Otras acciones complementarias que resulten necesarias.

8.6. Tratamiento de los informes de auditoría

Los informes de resultados de auditoría se entregan al Comité de Seguridad en un plazo máximo de 15 días tras la ejecución de la auditoría.

9. Requisitos comerciales y legales

9.1. Tarifas

9.1.1. Tarifa de emisión o renovación de certificados

Bit4id puede establecer una tarifa por la emisión o por la renovación de los certificados, de la que, en su caso, se informará oportunamente a los suscriptores.

9.1.2. Tarifa de acceso a certificados

Bit4id no ha establecido ninguna tarifa por el acceso a los certificados.

9.1.3. Tarifa de acceso a información de estado de certificado

Bit4id no ha establecido ninguna tarifa por el acceso a la información de estado de certificados.

9.1.4. Tarifas de otros servicios

Sin estipulación.

9.1.5. Política de reintegro

Sin estipulación.

9.2. Capacidad financiera

Bit4id dispone de recursos económicos suficientes para mantener sus operaciones y cumplir sus obligaciones, así como para afrontar el riesgo de la responsabilidad por daños y perjuicios, en relación a la gestión de

la finalización de los servicios y plan de cese, conforme a la legislación aplicable y normativa dictada por la AAC.

9.2.1. Cobertura de seguro

Se dispone de una garantía de cobertura de su responsabilidad civil suficiente, mediante un seguro de responsabilidad civil profesional, que mantiene de acuerdo a la normativa vigente aplicable.

9.2.2. Otros activos

Sin estipulación.

9.2.3. Cobertura de seguro para suscriptores y terceros que confían en certificados

Se dispone de una garantía de cobertura de su responsabilidad civil suficiente, mediante un seguro de responsabilidad civil profesional, para los servicios electrónicos de certificación.

9.3. Confidencialidad

9.3.1. Informaciones confidenciales

Las siguientes informaciones son mantenidas confidenciales:

- Solicitudes de certificados, aprobadas o denegadas, así como toda otra información personal obtenida para la expedición y mantenimiento de certificados, excepto las informaciones indicadas en la sección siguiente.
- Claves privadas generadas y/o almacenadas por la Entidad de Certificación.
- Registros de transacciones, incluyendo los registros completos y los registros de auditoría de las transacciones.
- Registros de auditoría interna y externa, creados y/o mantenidos por la Autoridad de Certificación y sus auditores.

- Planes de continuidad de negocio y de emergencia.
- Planes de seguridad.
- Documentación de operaciones, archivo, monitorización y otros análogos.
- Toda otra información identificada como "Confidencial".

9.3.2. Informaciones no confidenciales

La siguiente información se considera no confidencial:

- Los certificados emitidos o en trámite de emisión.
- La vinculación del suscriptor a un certificado emitido por la Entidad de Certificación.
- El nombre y los apellidos de la persona natural identificada en el certificado, así como cualquiera otra circunstancia o dato personal del titular, en el supuesto de que sea significativa en función de la finalidad del certificado.
- La dirección de correo electrónico de la persona natural identificada en el certificado, o la dirección de correo electrónico asignada por el suscriptor, en el supuesto de que sea significativa en función de la finalidad del certificado.
- Los usos y límites económicos reseñados en el certificado.
- El periodo de validez del certificado, así como la fecha de emisión del certificado y la fecha de caducidad.
- El número de serie del certificado.
- Los diferentes estados o situaciones del certificado y la fecha del inicio de cada uno de ellos, en concreto: pendiente de generación y/o entrega, válido, revocado, suspendido o caducado y el motivo que provocó el cambio de estado.
- Las listas de revocación de certificados (LRCs), así como las restantes informaciones de estado de revocación.
- La información contenida en los depósitos de certificados.
- Cualquier otra información que no esté indicada en la sección anterior.

9.3.3. Divulgación de información de suspensión y revocación

Véase la sección anterior.

9.3.4. Divulgación legal de información

Bit4id divulga la información confidencial únicamente en los casos legalmente previstos.

En concreto, los registros que avalan la fiabilidad de los datos contenidos en el certificado serán divulgados en caso de ser requerido para ofrecer evidencia de la certificación en un procedimiento judicial, incluso sin consentimiento del suscriptor del certificado.

Se indicarán estas circunstancias en la política de privacidad prevista en la sección 9.4.

9.3.5. Divulgación de información por petición de su titular

Se incluye, en la política de privacidad prevista en la sección 9.4, prescripciones para permitir la divulgación de la información del suscriptor y, en su caso, de la persona natural identificada en el certificado, directamente a los mismos o a terceros.

9.3.6. Otras circunstancias de divulgación de información

Sin estipulación.

9.4. Protección de datos personales

Bit4id garantiza el cumplimiento de la normativa vigente en cada momento en materia de protección de datos personales, reflejada en la Ley nº29733 de protección de datos personales y su Reglamento, así como la Norma Marco sobre Privacidad APEC. En cumplimiento de la

misma, Bit4id ha documentado en esta Declaración de Prácticas de Certificación y en su Plan de Privacidad, todos los aspectos y procedimientos de seguridad correspondientes.

Se utilizarán los datos de los usuarios, única y exclusivamente para los fines que figuran en esta Declaración de Prácticas de Certificación y de acuerdo con el Plan de Privacidad.
No se divulgan ni ceden datos personales, excepto en los casos previstos en las secciones 9.3.2 a 9.3.6, y en la sección 5.8, en caso de terminación del servicio de certificación.

La información confidencial de acuerdo con la normativa en protección de datos personales se protege mediante la aplicación de medidas de seguridad que garantían la protección de los datos de los usuarios frente a su alteración, pérdida, destrucción, daño, falsificación y procesamiento ilícito o no autorizado, de conformidad con las prescripciones establecidas en este documento y en la normativa de referencia.

9.5. Derechos de propiedad intelectual

9.5.1. Propiedad de los certificados e información de revocación

Bit4id goza de derechos de propiedad intelectual sobre los certificados que emita, sin perjuicio de los derechos de los suscriptores, poseedores de claves y terceros, a los que conceda licencia no exclusiva para reproducir y distribuir certificados, sin coste alguno, siempre y cuando la reproducción sea íntegra y no altere elemento alguno del certificado, y sea necesaria en relación con firmas digitales y/o sistemas de cifrado dentro del ámbito de uso del certificado, y de acuerdo con la documentación que los vincula.

Adicionalmente, los certificados emitidos por Bit4id contienen un aviso legal relativo a la propiedad de los mismos.

Las mismas reglas resultan de aplicación al uso de la información de revocación de los certificados.

9.5.2. Propiedad de la Declaración de Prácticas de Certificación

Bit4id goza de derechos de propiedad intelectual sobre esta Declaración de Prácticas de Certificación.

9.5.3. Propiedad de la información relativa a nombres

El suscriptor y, en su caso, la persona natural identificada en el certificado, conserva la totalidad de derechos, de existir los mismos, sobre la marca, producto o nombre comercial contenido en el certificado.

El suscriptor es el propietario del nombre distinguido (DN) del certificado, formado por las informaciones especificadas en la sección 3.1.1.

9.5.4. Propiedad de claves

Los pares de claves son propiedad de los suscriptores de los certificados.

Cuando una clave se encuentra fraccionada en partes, todas las partes de la clave son propiedad del propietario de la clave.

9.6. Obligaciones y responsabilidad civil

9.6.1. Obligaciones de Bit4id

Bit4id garantiza, bajo su plena responsabilidad, que cumple con la totalidad de los requisitos establecidos en la Declaración de Prácticas de Certificación, siendo el responsable del cumplimiento de los procedimientos descritos, de acuerdo a las indicaciones contenidas en este documento.

Se prestan los servicios de certificación conforme a esta Declaración de Prácticas de Certificación.

Con anterioridad a la emisión y entrega del certificado al suscriptor se informa al suscriptor de los términos y condiciones relativos al uso del certificado y de sus limitaciones de uso, mediante un contrato de suscriptor que incorpora por referencia los textos de divulgación (PDS) de los certificados adquiridos.

El documento de texto de divulgación, también denominado PDS[3], cumple el contenido del anexo A de la ETSI EN 319 411-1 v1.1.1 (2016-02), documento el cual puede ser transmitido por medios electrónicos, empleando un medio de comunicación duradero en el tiempo, y en lenguaje comprensible.

Bit4id vincula a suscriptores, poseedores de claves y terceros que confían en certificados, mediante dicho texto de divulgación o PDS, en lenguaje escrito y comprensible, con los siguientes contenidos mínimos:

- Prescripciones para dar cumplimiento a lo establecido en esta Declaración de Prácticas de Certificación.
- Indicación de la política aplicable, con indicación de que los certificados no se expiden al público.
- Manifestación de que la información contenida en el certificado es correcta, excepto notificación en contra por el suscriptor.
- Consentimiento para la publicación del certificado en el depósito y acceso por terceros al mismo.
- Consentimiento para el almacenamiento de la información empleada para el registro del suscriptor y para la cesión de dicha información a terceros, en caso de terminación de operaciones de la Entidad de Certificación sin revocación de certificados válidos.
- Límites de uso del certificado.

[3] "PKI Disclosure Statement", o declaración de divulgación de PKI aplicable.

- Información sobre cómo validar un certificado, incluyendo el requisito de comprobar el estado del certificado, y las condiciones en las cuales se puede confiar razonablemente en el certificado, que resulta aplicable cuando el suscriptor actúa como tercero que confía en el certificado.
- Forma en que se garantiza la responsabilidad patrimonial de la Entidad de Certificación.
- Limitaciones de responsabilidad aplicables, incluyendo los usos por los cuales la Entidad de Certificación acepta o excluye su responsabilidad.
- Periodo de archivo de información de solicitud de certificados.
- Periodo de archivo de registros de auditoría.
- Procedimientos aplicables de resolución de disputas.
- Ley aplicable y jurisdicción competente.
- Si la Entidad de Certificación ha sido declarada conforme con la política de certificación y, en su caso, de acuerdo con qué sistema.

9.6.2. Garantías ofrecidas a suscriptores y terceros que confían en certificados

Bit4id en la documentación que la vincula con suscriptores y terceros que confían en certificados, establece y rechaza garantías, y limitaciones de responsabilidad aplicables.

Bit4id, como mínimo, garantiza al suscriptor:

- Que no hay errores de hecho en las informaciones contenidas en los certificados, conocidos o realizados por la Autoridad de Certificación de Certificación.
- Que no hay errores de hecho en las informaciones contenidas en los certificados, debidos a falta de la diligencia debida en la gestión de la solicitud de certificado o en la creación del mismo.
- Que los certificados cumplen con todos los requisitos materiales establecidos en la Declaración de Prácticas de Certificación.

- Que los servicios de revocación y el empleo del Depósito cumplen con todos los requisitos materiales establecidos en la Declaración de Prácticas de Certificación.

Bit4id, como mínimo, garantizará al tercero que confía en el certificado:

- Que la información contenida o incorporada por referencia en el certificado es correcta, excepto cuando se indique lo contrario.
- En caso de certificados publicados en el Depósito, que el certificado ha sido emitido al suscriptor identificado en el mismo y que el certificado ha sido aceptado, de acuerdo con esta Declaración de Prácticas de Certificación.
- Que en la aprobación de la solicitud de certificado y en la emisión del certificado se han cumplido todos los requisitos materiales establecidos en la Declaración de Prácticas de Certificación.
- La rapidez y seguridad en la prestación de los servicios, en especial de los servicios de revocación y Depósito.

Adicionalmente, Bit4id garantiza al suscriptor y al tercero que confía en el certificado:

- Que, en el caso de que genere las claves privadas del suscriptor o, en su caso, persona natural identificada en el certificado, se mantiene su confidencialidad durante el proceso.
- La responsabilidad de la Entidad de Certificación, con los límites que se establezcan.

9.6.3. Rechazo de otras garantías

Bit4id rechaza toda otra garantía que no sea legalmente exigible, excepto las contempladas en la sección 9.6.2.

9.6.4. Limitación de responsabilidades

Bit4id limita su responsabilidad a la emisión y gestión de certificados y de pares de claves de suscriptores suministrados por la Entidad de Certificación.

9.6.5. Cláusulas de indemnidad

9.6.5.1. Cláusula de indemnidad de suscriptor

Bit4id incluye en el contrato con el suscriptor, una cláusula por la cual el suscriptor se compromete a mantener indemne a la Entidad de Certificación de todo daño proveniente de cualquier acción u omisión que resulte en responsabilidad, daño o pérdida, gasto de cualquier tipo, incluyendo los judiciales y de representación letrada en que pueda incurrir, por la publicación y uso del certificado, cuando concurra alguna de las siguientes causas:

- Falsedad o manifestación errónea realizada por el usuario del certificado.
- Error del usuario del certificado al facilitar los datos de la solicitud, si en la acción u omisión medió dolo o negligencia con respecto a la Entidad de Certificación o a cualquier persona que confía en el certificado.
- Negligencia en la protección de la clave privada, en el empleo de un sistema fiable o en el mantenimiento de las precauciones necesarias para evitar el compromiso, la pérdida, la divulgación, la modificación o el uso no autorizado de dicha clave.
- Empleo por el suscriptor de un nombre (incluyendo nombres comunes, dirección de correo electrónico y nombres de domino), u otras informaciones en el certificado, que infrinja derechos de propiedad intelectual o industrial de terceros.

9.6.5.2. Cláusula de indemnidad de tercero que confía en el certificado

Bit4id incluye en el texto de divulgación o PDS, una cláusula por la cual el tercero que confía en el certificado se compromete a mantener indemne a la Entidad de Certificación de todo daño proveniente de cualquier acción u omisión que resulte en responsabilidad, daño o pérdida, gasto de cualquier tipo, incluyendo los judiciales y de representación letrada en que pueda incurrir, por la publicación y uso del certificado, cuando concurra alguna de las siguientes causas:

- Incumplimiento de las obligaciones del tercero que confía en el certificado.
- Confianza temeraria en un certificado, a tenor de las circunstancias.
- Falta de comprobación del estado de un certificado, para determinar que no se encuentra suspendido o revocado.

9.6.6. Caso fortuito y fuerza mayor

Bit4id incluye en el texto de divulgación o PDS, cláusulas que limitan su responsabilidad en caso fortuito y en caso de fuerza mayor.

9.6.7. Ley aplicable

Bit4id establece, en el contrato de suscriptor y en el texto de divulgación o PDS, que la ley aplicable a la prestación de los servicios, incluyendo la política y prácticas de certificación, es la Ley Peruana.

9.6.8. Cláusulas de divisibilidad, supervivencia, acuerdo íntegro y notificación

Bit4id establece, en el contrato de suscriptor, y en el texto de divulgación o PDS, cláusulas de divisibilidad, supervivencia, acuerdo íntegro y notificación:

- En virtud de la cláusula de divisibilidad, la invalidez de una cláusula no afectará al resto del contrato.

- En virtud de la cláusula de supervivencia, ciertas reglas continuarán vigentes tras la finalización de la relación jurídica reguladora del servicio entre las partes. A este efecto, la Entidad de Certificación vela porque, al menos los requisitos contenidos en las secciones relativas a Obligaciones y responsabilidades, Auditoría y 9.3 Confidencialidad, continúen vigentes tras la terminación del servicio y de las condiciones generales de emisión/uso.
- En virtud de la cláusula de acuerdo íntegro se entenderá que el documento jurídico regulador del servicio contiene la voluntad completa y todos los acuerdos entre las partes.
- En virtud de la cláusula de notificación se establecerá el procedimiento por el cual las partes se notifican hechos mutuamente.

9.6.9. Cláusula de jurisdicción competente

Bit4id establece, en el contrato de suscriptor y en el texto de divulgación o PDS, una cláusula de jurisdicción competente, indicando que la competencia judicial internacional corresponde a los jueces peruanos.

La competencia territorial y funcional se determinará en virtud de las reglas de derecho internacional privado y reglas de derecho procesal que resulten de aplicación.

9.6.10. Resolución de conflictos

Bit4id establece, en el contrato de suscriptor, y en el texto de divulgación o PDS, los procedimientos de mediación y resolución de conflictos aplicables.

10. 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
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
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