BIT4ID SAC

DECLARACIÓN DE PRÁCTICAS DE REGISTRO O DE VERIFICACIÓN

Información general

Control documental

Clasificación de seguridad:	Público
Entidad de destino:	BIT4ID SAC
Versión:	2.6
Fecha edición:	24/08/2020
Fichero:	BIT4IDSAC_Práctica de registro_v2.6
Formato:	Office

Estado formal

Preparado por:	Revisado por:	Aprobado por:
Nombre: Alejandro Grande Fecha: 24/08/2020	Nombre: Albert Borrás Fecha: 24/08/2020	Nombre: Jorge García Fecha: 24/08/2020

Control de versiones

Versión	Partes que cambian	Descripción del cambio	Autor del cambio	Fecha del cambio
1.0	Original	Creación del documento	DMP/RLG	23/09/2016
2.0	íntegro	Adaptación completa del documento de acuerdo con la EC vinculada	ABD/DMP	15/01/2018
2.1	8.3	Se ha agregado detalles sobre la revocación	ABD	19/06/2018
2.2	íntegro	Adecuación conforme a las observaciones de la auditoría de INDECOPI	ABD	29/06/2018
2.3	2, 3, 5 y 9	Revisión del documento y ajuste al nuevo marco de la política de registro para la emisión de certificados digitales de acuerdo con la última guía de INDECOPI.	ABD	15/07/2019
2.4	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	08/07/2020
2.5	6.3, 6.4, 7.1, 8.3.4, 8.4.6, 8.4.8 y 8.4.9.	Adición de las entidades de certificación vinculadas a la ER. Se añaden tiempos de procesamiento respecto de la re-emisión y suspensión. Se añade periodo máximo respecto de un certificado suspendido. Se añade procedimiento de aprobación de solicitud de suspensión. Se añade apartado respecto de la vigencia de versiones.	AGB	20/08/2020
2.6	8.4.3 y 8.4.4	Se añade apartado referente a la aprobación y denegación de la solicitud de revocación Se añade tiempo de procesamiento de la solicitud de revocación, así como el tiempo de ejecución, en el mismo apartado.	AGB	24/08/2020

ÍNDICE

1. Introducción

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.

2. PARTICIPANTES

Son considerados como participantes, para efectos del presente documento, la entidad de certificación, la entidad de registro, los titulares y/o suscriptores, los terceros de confianza y los proveedores de servicios de valor añadido dentro de la IOFE y terceros contratistas que realizan funciones de registro.

2.1. Entidad de Certificación (EC)

La EC es la 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.

2.2. Entidad de Registro o Verificación (ER)

La 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.

2.3. Titulares y/o Suscriptores

La comunidad de usuarios definidos como titulares de los certificados digitales será definida según lo establecido en la Política de Certificación y Declaración de Prácticas de la Autoridad de Certificación. BIT4ID brinda servicios solamente a personas naturales o jurídicas. En el caso de personas naturales, los servicios de validación serán brindados a personas sin impedimento legal de nacionalidad peruana

2.4. Terceros de confianza

Los terceros que confían son personas naturales o jurídicas que confían en el contenido y la aplicación de un certificado digital. En este sentido, los terceros que confían pueden ser todas aquellas personas naturales y jurídicas que requieren evaluar la validez de un certificado para proceder con sus respectivas transacciones electrónicas, incluyendo entidades de otras infraestructuras además de la IOFE.

2.5. Terceros contratistas

Los terceros contratistas son personas naturales o jurídicas que realizan funciones de registro, tales como solicitudes de emisión, revocación, re-emisión, etc. En concreto serán los encargados 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.
- Si fuera necesario, gestionar la generación de claves y la emisión del certificado
- Hacer entrega del certificado al suscriptor o de los medios para su generación.
- Custodiar temporalmente de manera segura la documentación relativa a la identificación y registro de los firmantes y/o suscriptores y gestión del ciclo de vida de los certificados.
- Enviar de manera segura la documentación relativa al ciclo de vida de los certificados a las oficinas de la ER para su debida custodia y archivo.

Podrán actuar como terceos contratistas de BIT4ID cualquier entidad debidamente autorizada mediante la formalización de un contrato en el que se regularán las relaciones entre cada una de las partes.

Los terceros contratistas quedan sujetos al presente documento, en concreto a los mismos requisitos de seguridad y procedimientos propios de una ER, así como a la Política de seguridad de la Entidad de Registro que rige las funciones de registro.

3. DEFINICIONES Y ABREVIACIONES

Entidades 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.
Entidades de Registro o Verificación (ER)	Persona jurídica, con excepción de los notarios públicos, encargada del levantamiento de datos, la comprobación de éstos respecto a un solicitante de un certificado digital, la aceptación y autorización de las solicitudes para la emisión de un certificado digital, así como de la aceptación y autorización de las solicitudes de cancelación de certificados digitales. Las personas encargadas de ejercer la citada función serán supervisadas y reguladas por la normatividad vigente.
Declaración de Prácticas de Registro (RPS)	Conjunto de declaraciones sobre políticas y prácticas de la Entidad de Registro, que sirve para comunicar el cumplimiento legal y regulatorio a los suscriptores y terceros que confían.
Operador de Registro	Persona responsable de representar a la ER en las actividades de recepción, validación y procesamiento de solicitudes.
Prácticas de Registro	Son las prácticas que establecen las actividades y requerimientos de seguridad y privacidad correspondientes al Sistema de Registro o Verificación de una Entidad de Registro o Verificación.
Roles de confianza	Roles que tienen acceso a la información crítica de las operaciones de registro.
Suscriptor	Es la persona natural responsable de la generación y uso de la clave privada, a quien se le vincula de manera exclusiva con un documento electrónico firmado digitalmente utilizando su clave privada. En el caso que el titular del certificado digital sea una persona natural, sobre ella recaerá la responsabilidad de suscriptor. En el caso que una persona jurídica sea el titular de un certificado digital, la responsabilidad de suscriptor recaerá sobre el representante legal designado por esta entidad. Si el certificado está designado para ser usado por un agente automatizado, la titularidad del certificado y de las firmas digitales generadas a partir de dicho certificado corresponderán a la persona jurídica. La atribución de

	responsabilidad de suscriptor, para tales efectos, corresponde a la misma persona jurídica.
Tercero que confía	Se refiere a las personas naturales, equipos, servicios o cualquier otro ente que actúa basado en la confianza sobre la validez de un certificado y/o verifica alguna firma digital en la que se utilizó dicho certificado.
Titular	Es la persona natural o jurídica a quien se le atribuye de manera exclusiva un certificado digital.
Terceros contratistas	Los terceros contratistas son personas naturales o jurídicas que realizan funciones de registro, tales como solicitudes de emisión, revocación, re-emisión, etc.

4. USO APROPIADO DEL CERTIFICADO

Los criterios para definir el uso apropiado, rango de acción o aplicabilidad de un certificado digital solicitado a BIT4ID en calidad de ER, dependerán de lo establecido en la Política de Certificación y Declaración de Prácticas de cada Entidad de Certificación para las que BIT4ID brinda el servicio de ER.

5. ADMINISTRACIÓN DE POLÍTICAS

5.1. Organización que administra los documentos de RPS

La persona responsable de la administración de los servicios de certificación digital, es ubicable mediante la siguiente información de contacto:

- Nombre: JORGE GARCÍA ALIAGA
- Cargo: Gerente
- Dirección de correo electrónico: info.pe@uanataca.com

La política de Registro de BIT4ID y toda la documentación pertinente y relevante vigente de la Entidad de Registro, así como sus versiones anteriores, son publicadas en la siguiente dirección web: https://www.uanataca.com/pe.

Frente a cada modificación sobre el RPS de BIT4ID se publicará tan pronto como razonablemente sea posible.

5.2. Procedimiento de aprobación de RPS

BIT4ID a través de su responsable identificado en este documento aprueba su Declaración de Prácticas de Registro y Verificación, así como sus modificaciones y versiones, de acuerdo con el marco normativo de la IOFE.

5.3. Datos de la Entidad de Registro

Nombre: Bit4id S.A.C
Dirección: Oficina / Sede principal: Av. Antonio Miroquesada 360 Piso 4 Oficina 112 (Edificio WeWork), Magdalena del Mar, Lima
Correo electrónico: info.pe@uanataca.com
Página web: www.uanataca.com/pe

6. PUBLICACIÓN Y REGISTRO

6.1. Publicación de la información sobre certificación

La Declaración de Prácticas de Registro y toda la documentación pertinente y relevante vigente de BIT4ID en calidad de ER, así como sus versiones anteriores, son publicadas en la siguiente dirección web: https://www.uanataca.com/pe.

6.2. Tiempo o frecuencia de la publicación

Las modificaciones relativas a la RPS u otra documentación de la ER de BIT4ID, deben ser publicadas tan pronto como razonablemente sea posible, debiendo tener cuidado de cumplir con los requisitos que fueren necesarios para la aprobación de dichas modificaciones.

6.3. Vigencia de la versión documental actual

Este documento es el único vigente, quedando sin efecto versiones anteriores del mismo.

6.4. Controles de acceso a los registros

El acceso a los registros es restringido únicamente para el uso de los titulares y suscriptores legítimos, así como a los trabajadores competentes dentro de la ER, teniendo en cuenta los temas de privacidad que pudieran existir en los contratos de los suscriptores o titulares de conformidad con la Norma Marco sobre Privacidad.

La ER debe emplea sistemas fiables para el registro, de modo tal que:

- Únicamente personas autorizadas tengan acceso a lectura y modificaciones.
- Pueda comprobarse la autenticidad de la información.

7. IDENTIFICACIÓN Y AUTENTICACIÓN

BIT4ID establece procedimientos para seguros para garantizar la posesión de la clave privada, conformes con los estándares de seguridad Common Criteria EAL 4+ y/o FIPS 140-2 de acuerdo a la guía de acreditación de la ACC. En este sentido, BIT4ID implementa procedimientos conformes a la legislación aplicable para la autenticación de la identidad de personas físicas y jurídicas, en la solicitud de emisión y remisión de certificados, estableciendo procedimientos análogos que les permita la suspensión y revocación de los mismos. BIT4ID declara verificar documental y/o telemáticamente todos los datos que incluye en los certificados emitidos.

Para lo anterior, BIT4ID desarrolla su respectiva declaración de prácticas de registro basada en los procedimientos mencionado en el párrafo precedente, siempre de conforme a la normativa de aplicación, y la Declaración de Prácticas de Certificación de la Entidad de Certificación a la cual se encuentra vinculada.

7.1. Entidades de Certificación Vinculadas a la Entidad de Registro

Atendiendo al criterio de la autoridad competente, se expresa una lista de las entidades de certificación que se encuentran vinculadas a la Entidad de Registro de BIT4ID, en adelante Entidades Vinculadas:

- La Entidad de Certificación de Bit4id S.A.C.

7.2. Reconocimiento, autenticación y rol de las marcas registradas

Se prohíbe a los solicitantes de certificados de personas jurídicas que incluyan nombres en las solicitudes que puedan suponer infracción de derechos de terceros.

En el caso de personas jurídicas, no se podrá volver a asignar un nombre de titular que ya haya sido asignado a un titular diferente.

No le corresponde a la ER determinar si un solicitante de certificados le asiste algún tipo de derecho sobre el nombre que aparece en una solicitud de certificado. Asimismo, no le corresponde resolver ninguna disputa concerniente a la propiedad de nombres de personas naturales o jurídicas, nombres de dominio, marcas o nombres comerciales. Sin embargo, la ER debe cerciorarse mediante la validación de la documentación e información requerida del solicitante del certificado que tanto el nombre del titular como del suscriptor correspondan a los solicitantes.

La ER tiene el derecho de rechazar una solicitud de certificado a causa de conflicto de nombres.

7.3. Validación inicial de la identidad

7.3.1. Método para probar la posesión de la clave privada

Si una EC vinculada a la ER de BIT4ID establece en su CPS o CP que el par de claves sea generado en las instalaciones de la ER, ésta debe demostrar el control exclusivo sobre la clave privada, en virtud del procedimiento fiable de emisión, de entrega y de aceptación del dispositivo de creación de firma, del correspondiente certificado y el par de claves almacenados en su interior, conforme a lo estipulado en la CPS de la EC. En cualquier otro caso, el procedimiento se regirá por lo previsto en las CPS y CP de la EC vinculada.

7.3.2. Autenticación de la identidad de una persona jurídica

El proceso de comprobación de la identidad de la persona jurídica cuyos datos se incluyen en un certificado tiene como objetivo garantizar que el suscriptor y el titular sean las mismas personas identificadas en la solicitud de emisión de un certificado, y que la información que se incluya en el certificado sea verdadera y exacta. Para ello, la ER requiere al solicitante del certificado, presentarse personalmente, llevando la documentación correspondiente.

El personal asignado por la ER, deberá validar la identidad del solicitante, para ello la ER debe establecer los procedimientos de validación considerando los requerimientos de la normativa aplicable:

- El Representante Legal o una persona asignada por él deberá acreditar la existencia de la persona jurídica y su vigencia mediante los instrumentos públicos o norma legal respectiva, así como sus facultades como representante. Para ello, es preciso presentar un documento público o escritura que acredite dicha representación. Este requisito de presentación de documento público podrá ser omitido en caso de que la ER pueda realizar consultas telemáticas para comprobar la vigencia de la representación que alega tener el solicitante.
- La existencia y vigencia de la persona jurídica deberá acreditarse con el documento de vigencia respectivo expedido por los Registros Públicos o mediante la especificación de la norma legal de creación de la persona jurídica correspondiente. En el caso de empresas constituidas en el extranjero, se acreditará su existencia y vigencia mediante un certificado de vigencia de la sociedad u otro instrumento equivalente expedido por la autoridad competente en su país de origen.

  La exigencia de presentar la documentación a que hace referencia el párrafo anterior, podrá ser omitida en caso de que la ER pueda realizar consulta telemática a través de las que pueda verificar la información relativa a la existencia de la persona jurídica.
- El Representante Legal de la persona jurídica o una persona asignada por él, deberá firmar un contrato, que en adelante llamaremos “contrato del titular”. A través de dicho contrato, el titular deberá declarar tener conocimiento de los términos y condiciones aplicables a los certificados.
- Si fuera el caso, los responsables de realizar las solicitudes de certificados, en representación de la persona jurídica, deben enviar las solicitudes a través de medios no repudiables.
- Los aspirantes a suscriptores deben presentarse a la ER. El proceso de verificación de sus identidades debe cumplir los requerimientos establecidos en el presente documento respecto de la autenticación de personas naturales.
- Tratándose de certificados digitales solicitados por personas jurídicas para su utilización a través de agentes automatizados, se deberá acreditar la existencia

de la persona jurídica y la identidad de la persona responsable sobre dicho agente automatizado. La titularidad de certificados y de las firmas digitales generadas a partir de dicho certificado corresponderá a la persona jurídica de acuerdo a las políticas de certificación de la EC. La atribución de responsabilidad, para tales efectos, corresponde al representante legal, que en nombre de la persona jurídica solicita el certificado digital.

- En general cualquier documento que se requiera aportar para acreditar requisitos para la emisión de certificados, podrá ser cumplido mediante la consulta telemática a registros públicos y/o privados por parte de la ER.

7.3.3. Autenticación de la identidad de persona natural

El proceso de comprobación de la identidad de la persona natural cuyos datos se incluyen en un certificado tiene como objetivo garantizar que el titular sea la misma persona identificada en la solicitud de emisión de un certificado, y que la información que se incluya en el certificado sea verdadera y exacta. Para ello, la ER debe requerir al solicitante del certificado, presentarse personalmente, llevando la documentación establecida en la RPS o CPS según sea el caso.

El personal asignado por la ER, deberá validar la identidad del solicitante, para ello la ER establece procedimientos de validación de los soportes de acuerdo a la normativa aplicable.

- La ER verifica la identidad del solicitante mediante la verificación del original de un documento oficial de identidad, el mismo que deberá estar en vigor en la fecha de realización del proceso de registro.
- La información proporcionada por los solicitantes es validada por la ER a través de un mecanismo de consulta confiable, como es el caso de las bases de datos nacionales o registros públicos.

7.3.4. Información no verificada del suscriptor

De manera general, no se incluye en los certificados, información no verificada del suscriptor o el titular según sea el caso. La IOFE permite una excepción en el caso de la dirección de correo electrónico del suscriptor. En este caso se debe comprobar que la

dirección de correo electrónico que se incluye en el certificado es la que efectivamente desea incluir el solicitante. La ER no está obligada a comprobar ni la existencia de la cuenta de correo electrónico indicada por el solicitante, ni que la dirección sea única, ni su correcto funcionamiento, todo lo cual es responsabilidad del solicitante.

7.3.5. Validación de la autoridad

Cuando un individuo solicita la emisión de un certificado que sirva para acreditar el ejercicio de un cargo en concreto, la ER requiere a este solicitante las pruebas que evidencien su cargo, incluyendo la facultad de actuar en nombre de la persona jurídica en la que ocupa dicho cargo. El requerimiento de este documento puede ser cumplido mediante consulta telemática al registro público o privado donde se encuentre la información que acredita el carácter del solicitante.

7.4. Identificación y autenticación para solicitudes de re-emisión de certificado

BIT4ID de acuerdo a las CPS de su EC vinculada, informa a sus suscriptores la posibilidad de re-emisión de los certificados.

7.4.1. Identificación y Autenticación para solicitudes de remisión de certificados rutinaria

La re-emisión rutinaria puede producirse cuando la fecha la fecha de su expiración es cercana y menor a un plazo máximo de un año. Sólo los titulares y suscriptores de certificados pueden solicitar la re-emisión de certificados, tanto en el caso de personas naturales como personas jurídicas.

La ER de BIT4ID utiliza los siguientes medios de verificación de la identidad del solicitante de la re-emisión del certificado:

- 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 solicitar su re-emisión.

Antes de aprobar la re-emisión el certificado con la nueva clave pública, la ER comprueba que la información del titular y del suscriptor contenida en el certificado continúa siendo válida, para lo cual podrá valerse documentación acreditativa que aporte el solicitante o bien de consultas telemáticas a bases de datos públicas o privadas que contengan la información correspondiente. Si cualquier información del titular o del suscriptor hubiere cambiado, se registrará adecuadamente la nueva información.

En los casos que el certificado del titular hubiera expirado o hubiera sido revocado, deberá seguirse el proceso para la emisión de un nuevo certificado y la validación de identificación inicial descrita en este documento.

Sólo se podrá realizar una única re-emisión de certificado. Luego de la expiración de un certificado re-emitido, se sigue el proceso para la emisión de un nuevo certificado y la validación de identificación inicial descrita en este documento.

7.4.2. Identificación y Autenticación para la re-emisión de certificado luego de la revocación

En el caso que el certificado del titular haya sido revocado, deberá seguirse el proceso de validación de identidad inicial, especificado en de este documento.

7.5. Identificación y autenticación para la solicitud de revocación

El suscriptor y el titular pueden tramitar solicitar a la EC o ER la revocación de su certificado a través de medios telemáticos utilizando un medio que garantice el no repudio, como un mensaje firmado con un certificado válido, código de revocación, la

autenticación a través de una frase secreta conocida sólo por el suscriptor del certificado entre otro.

En el caso de solicitud presencial, la ER de BIT4ID:

- Los suscriptores deben presentar en la ER su documento oficial de identidad.
- Un representante asignado por la persona jurídica puede solicitar la revocación de los certificados de la entidad, para ello debe presentar a la ER, documentos que acrediten dicha representación y la voluntad de dicha persona jurídica.
- En caso de que la solicitud sea presentada por un tercero distinto al suscriptor y titular, este deberá presentar en la ER pruebas fehacientes del uso indebido del certificado de acuerdo con la ley vigente.
- La revocación puede ser también solicitada mediante una orden judicial, la cual debe ser recibida y procesada por la ER.

8. REQUISITOS OPERACIONALES DEL CICLO DE VIDA DE LOS CERTIFICADOS

El ciclo de vida de los certificados digitales lo determina la EC de acuerdo a sus CP y CPS. No obstante, BIT4ID como Entidad de Registro gestiona únicamente la emisión de certificados con una vigencia máxima no superior a la que establece la normativa aplicable.

8.1. Solicitud del certificado

Los procedimientos de solicitud dependerán de lo establecido en la CP y CPS de cada EC a la que BIT4ID se encuentra vinculada.

8.1.1. Habilitados para presentar la solicitud de un certificado

La solicitud en el caso de personas naturales debe ser hecha por la misma persona que pretende ser titular del certificado o por un representante que cuente con facultades expresas para tales efectos otorgadas mediante poder. En este caso, el titular del certificado será el poderdante y corresponderá al apoderado la condición de suscriptor. El ámbito de utilización del certificado digital en este supuesto, se encontrará circunscrito y limitado a las facultades expresamente conferidas en el poder.

En el caso de personas jurídicas, se pueden solicitar certificados de atributo para ser usados por funcionarios y personal específico, incluso por el Representante legal. En este caso, se considera como aspirante a titular del certificado a la persona jurídica y dichas personas naturales vienen a ser los aspirantes a suscriptor. El solicitante deberá especificar en su solicitud el tipo de atributo al que corresponderá el certificado.

La ER de BIT4ID gestionará en la gestión del certificado la emisión de un perfil que se corresponda con los atributos de un representante legal de la persona jurídica, en forma diferenciada de un perfil de certificado identifique a trabajadores, agentes o personas

vinculadas que como parte de su cargo requieren de un certificado digital, lo cual se advertirá al solicitante.

En el caso que el certificado esté destinado para ser usado por un agente automatizado, la solicitud debe ser hecha por un representante designado por la persona jurídica dueña del dispositivo. En este caso, la titularidad del certificado y de las firmas digitales generadas a partir de dicho certificado corresponderá a la persona jurídica. La atribución de responsabilidad, para tales efectos corresponde al representante legal, que en nombre de la persona jurídica solicita el certificado digital.

Un suscriptor puede efectuar solicitudes referentes a múltiples titulares, siempre y cuando exista entre las partes una relación de por medio que faculte al suscriptor para proceder de esa manera. Esta posibilidad podrá verse limitada de acuerdo a las CP y CPS a las que la ER de BIT4ID se encuentre vinculada.

8.1.2. Proceso de solicitud y responsabilidades

El proceso de solicitud y las responsabilidades asumidas por el uso del certificado, dependerán de lo establecido en las CP y CPS de cada EC a la que BIT4ID se encuentra vinculada.

8.2. Procesamiento de la solicitud de un certificado

8.2.1. Realización de las funciones de identificación y autenticación

La ER de BIT4ID utiliza los siguientes procedimientos de verificación para la validación de la identidad de una persona jurídica, natural o PSC:

a. Se requiere una entrevista presencial con el solicitante del certificado para la verificación de su identidad.
b. Se establece el lugar donde se realiza la verificación.
c. Se establece la persona responsable de la verificación.
d. Se determinan los documentos requeridos para identificar a una persona según la siguiente clasificación:
    1. Natural
    2. Jurídica

- Atributos
- Dispositivo para agente automatizado

3. PSC

e. Se establecen procedimientos para la validación de la documentación presentada por el solicitante del certificado para cada uno de los casos.

La de EC reconocerá la información de identificación de los suscriptores de las solicitudes proporcionadas por la ER.

Si las solicitudes son remitidas de manera electrónica, la ER debe realizar el correspondiente proceso de identificación y dicha solicitud debe ser firmada digitalmente por la ER empleando para tales efectos una clave de un certificado emitido por la EC u otra autoridad que haya sido reconocida por INDECOPI.

8.2.2. Aprobación o rechazo de la solicitud de certificado

Las solicitudes serán rechazadas si el solicitante no está capacitado para participar de la comunidad de usuarios de la IOFE, o si el resultado de la validación realizada por la ER fue negativo, conforme a lo establecido en este documento.

En caso de que la solicitud sea aprobada, la ER de BIT4ID procederá a:

- Comunicar a la EC su aprobación para la emisión del certificado a través de los canales seguros de comunicación para la generación del certificado.
- La ER emitirá el contrato del servicio que el suscriptor (o su representante) deberá firmar, el cual contendrá las obligaciones que garanticen el efecto legal de las transacciones realizadas con el certificado y las responsabilidades de su incumplimiento.

Las ECs con las que BIT4ID esté vinculada deben establecer el contenido del contrato del suscriptor en coordinación con esta ER, reflejando tanto las responsabilidades de la EC, la ER y la de los suscriptores y titulares; y los procedimientos a seguir para realizar la firma del mismo. La ER podrá emitir y archivar el contrato firmado de forma digital o manuscrita.

8.2.3. Tiempo para el procesamiento de la solicitud de un certificado

Una vez validada la información proporcionada por el suscriptor, si el resultado de la validación es positivo, la ER debe enviar a la EC la autorización de la emisión del certificado de manera inmediata, salvo que medie alguna razón justificada.

Las ECs con las que BIT4ID esté vinculada debe establecer en su CP u otra documentación relevante el tiempo necesario para el procesamiento de solicitudes, este tiempo no debe ser mayor a 5 días útiles a partir de la entrevista presencial del solicitante en la ER, considerando el intercambio de información necesario entre la EC y la ER.

8.3. Re-emisión de certificado

El proceso de re-emisión se encuentra regulado por las ECs a las que la ER se encuentra vinculada, de acuerdo a sus CP y CPS.

8.3.1. Circunstancias para la re-emisión de un certificado

La re-emisión de un certificado se realizará de acuerdo a las CPS de las ECs a las que se encuentre vinculada la ER de BIT4ID. En este proceso se generarán un nuevo par de claves y un nuevo certificado correspondiente a una nueva clave pública, pero manteniendo la mayor parte de la información del suscriptor contenida en el certificado a expirar, de acuerdo con lo establecido en este documento.

La re-emisión de claves rutinaria es un proceso programado cada vez que un nuevo par de claves debe ser emitido debido a su expiración y con anticipación a ésta. Siempre que una EC vinculada a BIT4ID brinde el servicio de re-emisión de certificados, se permitirá a los titulares solicitar una re-emisión rutinaria del mismo, antes de que ocurra la expiración de su certificado, siempre y cuando el periodo de vigencia restante de su certificado no sea mayor al plazo de un año.

En el caso que el certificado del titular haya expirado o haya sido revocado, deberá seguirse el proceso de identificación inicial ante la ER, descrito en el presente documento. Sólo se puede realizar una única re-emisión del certificado por un año adicional como

máximo. No será necesaria la identificación presencial para la re-emisión, de acuerdo a lo establecido en esta RPS.

8.3.2. Personas habilitadas para solicitar la reemisión de certificado

Sólo el titular de un certificado puede solicitar la reemisión de su certificado, en las condiciones indicadas en esta RPS.

La ER de BIT4ID únicamente aceptará solicitudes de re-emisión de certificados en representación de las ECs acreditadas, con las cuales mantiene un convenio para la prestación de servicios de certificación digital.

8.3.3. Procesamiento de las solicitudes para re-emisión de certificados

La solicitud de re-emisión de certificado será ser rechazada en caso que el periodo de uso del certificado o las claves haya expirado o sea mayor a un año, en este caso deberá seguirse el proceso inicial de verificación de identificación ante la ER.

Antes de aprobar la re-emisión de un certificado, la ER comprueba que la información utilizada para verificar la identidad y los restantes datos del titular y del suscriptor continúan siendo válidos. Si cualquier información del titular o del suscriptor ha cambiado, se registra adecuadamente la nueva información. La validación de la información se realizará de acuerdo a lo previsto en este documento. La solicitud de re-emisión será firmada por el solicitante.

Verificados los datos del titular, la ER de BIT4ID gestionará la re-emisión del certificado a la EC vinculada, notificando los datos de la solicitud y la aprobación de la misma, a través de los mecanismos que establezca la EC de acuerdo a sus CPS. La ER en la notificación envía copia de la solicitud de re-emisión firmada.

8.3.4. Tiempo de procesamiento de las solicitudes para re-emisión de certificados

Las solicitudes para re-emisión de certificados se procesarán por orden de llegada de forma inmediata. Si se realiza a través de un operador, se ejecutará dentro del horario

ordinario de operación de BIT4ID o en su caso de la Entidad de Registro. Si se realiza a través del servicio online, se realizará de forma inmediata.

8.4. Revocación y suspensión del certificado

8.4.1. Circunstancias para la revocación

El titular y el suscriptor del certificado están obligados, bajo responsabilidad, a solicitar la revocación al tomar conocimiento de la ocurrencia de alguna de las siguientes circunstancias:

- Por exposición, puesta en peligro o uso indebido de la clave privada.
- Por deterioro, alteración o cualquier otro hecho u acto que afecte la clave privada.
- Revocación de las facultades de representación y/o poderes de sus representantes legales o apoderados.
- Cuando la información contenida en el certificado ya no resulte correcta.
- Cuando el suscriptor deja de ser miembro de la comunidad de interés o se sustrae de aquellos intereses relativos a la EC.
- Cuando el suscriptor o titular incumple las obligaciones a las que se encuentra comprometido dentro de la IOFE a través de lo estipulado en el contrato del suscriptor y/o titular.
- Cuando la información contenida en el certificado ya no resulte correcta.
- Por decisión de la legislación respectiva.
- Por muerte, o por inhabilitación o incapacidad declarada judicialmente de la persona natural titular del certificado.

En caso de que los cambios en la información del titular no tengan impacto en los terceros que confían, es necesaria la revocación del certificado existente ni la emisión de uno nuevo.

8.4.2. Personas habilitadas para solicitar la revocación

De acuerdo con lo estipulado por la Ley, el tipo de personas que pueden solicitar la revocación de un certificado:

- El titular o suscriptor del certificado.
- La EC o ER que emitió el certificado.
- Un juez que de acuerdo con la Ley decida revocar el certificado.
- Un tercero que tenga pruebas fehacientes del uso indebido del certificado, el compromiso de clave u otro motivo de revocación mencionado en la Ley, los reglamentos de acreditación y el presente documento.

8.4.3. Aprobación o denegación de la solicitud de Revocación

En caso de que los datos se verifiquen correctamente, BIT4ID aprobará la solicitud de revocación del certificado. En el caso de que el solicitante no se encuentre capacitado para participar de la comunidad de usuarios de la IOFE por cualquiera de las causas descritas por la misma, o si la ER, al validar la identidad del individuo solicitante obtiene fundamento suficiente para negar dicha validación, se procederá al rechazo de la solicitud de revocación.

UANATACA notifica al solicitante la aprobación o denegación de la solicitud.

8.4.4. Tiempo de procesamiento de las solicitudes para revocación de certificados

Las solicitudes para revocación de certificados se procesarán por orden de llegada de forma inmediata. Si se realiza a través de un operador, se ejecutará dentro del horario ordinario de operación de BIT4ID o en su caso de la Entidad de Registro. Si se realiza a través del servicio online, se ejecutará de forma inmediata.

8.4.5. Procedimiento para la solicitud de revocación

El suscriptor y el titular pueden solicitar a la EC o ER la revocación de su certificado a través de medios telemáticos utilizando un medio que garantice el no repudio, como un mensaje firmado con un certificado válido, la autenticación a través de una frase secreta conocida sólo por el suscriptor del certificado, etc. El suscriptor también puede realizar la solicitud a la ER mediante una petición presencial. En todos los casos la solicitud de revocación deberá ser firmada por el solicitante.

La ER de BIT4ID, deja constancia de la identidad del solicitante, los motivos de la revocación y cualquier otra observación que resulte pertinente. En caso de que no se acepte la revocación, la ER deja constancia de los hechos que motivaron dicha denegatoria.

Los terceros (incluyendo órdenes judiciales) deben presentarse personalmente o mediante un representante legalmente autorizado en las instalaciones de la ER para realizar la solicitud de revocación, con la documentación que corresponda de acuerdo con estas RPS.

Las ECs vinculadas a BIT4ID establecen en sus CPS, el procedimiento para realizar las solicitudes de revocación de los certificados de los suscriptores.

Cuando se produzca la revocación, la misma indicará el momento desde la que se aplica, precisando la fecha, hora, minuto y segundo. La revocación no aplicará de manera retroactiva y se notificará al titular del certificado digital.

8.4.6. 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.

8.4.7. Personas habilitadas para solicitar la suspensión

Pueden solicitar la 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.

8.4.8. Período máximo de un certificado en estado suspendido

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

8.4.9. Procedimientos de solicitud de suspensión o reactivación

La persona o entidad que precise la suspensión de un certificado, puede solicitarlo a la Entidad de Registro o realizarlo él mismo a través del servicio online disponible en la página web de BIT4ID.

La solicitud de suspensión 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 suspensión.

8.4.10. Aprobación o rechazo de la solicitud de suspensión

En caso de que los datos se verifiquen correctamente, BIT4ID aprobará la solicitud de suspensión del certificado. En el caso de que el solicitante no se encuentre capacitado para participar de la comunidad de usuarios de la IOFE por cualquiera de las causas descritas por la misma, o si la ER, al validar la identidad del individuo solicitante obtiene fundamento suficiente para negar dicha validación, se procederá al rechazo de la solicitud de suspensión.

UANATACA notifica al solicitante la aprobación o denegación de la solicitud.

8.4.11. Tiempo de procesamiento de las solicitudes para suspensión de certificados

Las solicitudes para suspensión de certificados se procesarán por orden de llegada de forma inmediata. Si se realiza a través de un operador, se ejecutará dentro del horario ordinario de operación de BIT4ID o en su caso de la Entidad de Registro. Si se realiza a través del servicio online, se realizará de forma inmediata.

8.5. Modificación del certificados

De acuerdo con los procesos previstos con la EC a la que se encuentra vinculada, la ER de BIT4ID no prestará el servicio de modificación de certificados.

9. CONTROLES DE LAS INSTALACIONES, DE LA GESTION Y CONTROLES OPERACIONALES

Los presentes controles y requisitos de seguridad con respecto de las instalaciones, la gestión y controles operacionales se aplicarán según correspondan, a todas las entidades que realicen funciones de registro.

9.1. Controles físicos

9.1.1. Ubicación y construcción del local

Las instalaciones de ER BIT4ID cuentan con medidas razonables contra daños por desastres naturales, como inundación, terremoto; así como desastres creados por el hombre, como incendios, disturbios civiles y otras formas de desastre, que se documentan en Política de Seguridad.

9.1.2. Acceso físico

Todas las áreas sensibles cuentan con controles de acceso apropiados para garantizar que sólo se permita el acceso al personal autorizado. El registro y acceso a las áreas de la ER se regula de acuerdo con la política de seguridad de la ER.

9.1.3. Energía y aire acondicionado

Los equipos de energía y aire acondicionado están protegidos y en constante mantenimiento a efectos de asegurar su correcto funcionamiento. La instalación eléctrica y los equipos de aire acondicionado reciben mantenimientos anuales.

9.1.4. Exposición al agua

Las instalaciones están protegidas contra exposiciones al agua de acuerdo a lo que indica el certificado de inspección técnica de seguridad en edificaciones emitido por la correspondiente Municipalidad del distrito donde se ubican las sedes de Bit4Id SAC que considera la verificación de lo siguiente:

- Tuberías de agua fría, agua caliente, válvulas de control y/o accesorios en general se encuentran operativas y no presentan fugas de agua.
- Los depósitos de almacenamiento son de material resistente e impermeable, están dotados de los dispositivos necesarios y cuenta con rebose para su correcta operación y mantenimiento.

La red de colección no presenta fugas de agua y asegura la evacuación de las aguas servidas.

9.1.5. Prevención y protección contra fuego

Las instalaciones poseen adecuadas medidas para la prevención y protección contra el fuego de acuerdo a lo que indica el certificado de inspección técnica de seguridad en edificaciones emitido por la correspondiente Municipalidad del distrito donde se ubican las sedes de Bit4Id SAC que considera la verificación de lo siguiente:

- La edificación se encuentra protegida con un sistema de detección y alarma de incendios centralizado.
- El número de extintores es adecuado para el tipo de local y riesgo existente.

9.1.6. Archivo de material

Los archivos tanto electrónicos como de papel y el material en general, están protegidos contra accesos no autorizados y destrucción tanto deliberada como accidental, incluyendo destrucción por fuego, temperatura, agua, humedad y magnetismo.

Los soportes de información sensible se almacenan de forma segura en armarios contra fuegos, según el tipo de soporte y la clasificación de la información en ellos contenida, en diversas ubicaciones y su acceso se encuentra restringido.

9.1.7. Gestión de residuos

La ER posee procedimientos para la gestión y destrucción de residuos que garantizan la imposibilidad de recuperación de la información.

9.1.8. Copia de seguridad externa

Se disponen de copias de seguridad externa de toda la información sensible y de aquella considerada como necesaria para la persistencia de su actividad, las cuales se mantienen apropiadamente.

9.2. Controles procesales

9.2.1. Roles de confianza

BIT4ID ha identificado, de acuerdo con su política de seguridad, 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 proceso de registro. Las tareas de Auditor interno son incompatibles con el resto de roles de confianza
- **Operador de Registro:** Persona responsable de aprobar las peticiones de certificación realizadas por el suscriptor y emitir certificados digitales. Encargado de la emisión, revocación, renovación y suspensión del ciclo de vida de los certificados de los suscriptores. Asimismo es el encargado de realizar las tareas de identificación de acuerdo con las políticas y prácticas de UANATCA.
- **Responsable de Seguridad**: Encargado de coordinar, controlar y hacer cumplir las medidas de seguridad definidas por las políticas de seguridad de BIT4ID. 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.

9.2.2. Número de personas requeridas por labor

Se garantiza al menos dos personas para realizar las tareas relativas a la ejecución de tareas emisión, revocación, renovación y suspensión, en general para la gestión del ciclo de vida.

9.2.3. Identificación y autenticación para cada rol

El personal de la ER que accede a los sistemas para visualizar, modificar o realizar cualquier acción relativa a los servicios de certificación se autentica con certificado digital en tarjeta inteligente.

9.2.4. Roles que requieren funciones por separado

Los siguientes roles presentan separación de funciones:

- Auditor. Las tareas propias del rol de Auditor serán incompatibles con el resto de funciones fiables, incluidas con las operaciones y tareas de registro.
- Operador de registro. Las tareas del operador de registro son incompatibles con las Auditor interno.
- Responsable de seguridad. Las tareas del Responsable de Seguridad son incompatibles con las Auditor interno.

9.3. Controles de personal

La ER de BIT4ID establece dentro de este documento, en los contratos de servicio del personal y en documentación ad hoc, la aceptación del conocimiento sobre la confidencialidad y normativa de privacidad aplicable a la gestión los servicios de la ER.

9.3.1. Cualidades y requisitos, experiencia y certificados

Todo el personal está cualificado y/o ha sido instruido convenientemente para realizar las operaciones que le han sido asignadas. Asegurando que el personal de registro es confiable para realizar las tareas de registro.

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 un empleado 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 una función fiable a una persona que no sea idónea para el puesto, especialmente por una falta que afecte su idoneidad para el puesto. Por este motivo, previamente se realiza una investigación hasta donde permita la legislación aplicable, relativa a los siguientes aspectos:

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

9.3.2. Procedimiento para verificación de antecedentes

Con carácter previo a la contratación de a 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.

Para llevar a cabo la verificación, se obtiene el consentimiento inequívoco del afectado para dicha investigación previa, y se procesa y protege todos sus datos personales de acuerdo con la normativa vigente en concepto de protección de la privacidad de la información, en concreto a las obligaciones que derivan del decreto supremo n° 004-2007-PCM y de la norma marco sobre privacidad APEC.

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.

9.3.3. Requisitos de capacitación

La ER forma al personal en puestos fiables y de gestión, hasta que alcanzan la cualificación necesaria, manteniendo archivo de dicha formación.

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

La formación incluye, al menos, los siguientes contenidos:

- Principios y mecanismos de seguridad.
- Tareas que debe realizar la persona.
- Políticas y procedimientos de seguridad de la ER. 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.

9.3.4. Frecuencia y requisitos de las re-capacitaciones

BIT4ID, actualiza la formación del personal 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.

9.3.5. Frecuencia y secuencia de la rotación en el trabajo

No aplicable.

9.3.6. Sanciones por acciones no autorizadas

La ER 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.

9.3.7. Requerimientos de los contratistas

Los empleados contratados para realizar tareas confiables firman con anterioridad las cláusulas de confidencialidad y los requerimientos operacionales empleados. Cualquier acción que comprometa la seguridad de los procesos aceptados podría, una vez evaluados, dar lugar al cese del contrato laboral.

En el caso de que todos o parte de los servicios propios de una Entidad de Registro sean operados por un tercero, los controles y previsiones realizadas en esta sección, o en otras partes de esta Declaración de Prácticas de Registro, serán aplicados y cumplidos por el tercero que realice las funciones correspondientes. No obstante lo anterior, la entidad de registro 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 registro por tercero distinto a BIT4ID.

9.3.8. Documentación suministrada al personal

La ER suministrará la documentación que estrictamente precise su personal en cada momento, al objeto de realizar su trabajo de forma competente y satisfactoria.

El personal dispondrá de la documentación necesaria para el desempeño de sus funciones, que de manera orientativa pero no limitativa:

- Una declaración sobre sus funciones y autorizaciones.
- Manuales sobre procedimientos y herramientas necesarias para el despeño de sus funciones.

- Se tendrá acceso a las políticas que le sean de aplicación y en concreto a la política de seguridad y a la Declaración de Prácticas de Registro.
- Si fuese necesario, la legislación aplicable a sus funciones.
- Documentación respecto a sus roles frente a plan de contingencia.

9.4. Procedimiento de registro de auditorías

9.4.1. Tipos de eventos registrados

La ER registra información de auditoría sobre los eventos que pueden impactar en la seguridad de las operaciones:

- Encendido y apagado de los sistemas que procesan información sensible.
- Intentos de crear, borrar, cambiar contraseñas o permisos de los usuarios dentro del sistema que procesa información sensible.
- Intentos de entrada y salida del sistema que procesa información sensible.
- Intentos no autorizados de acceso a los registros o bases de datos del sistema.

Adicionalmente, se registra la siguiente información:

- Mantenimientos y cambios de configuración del sistema que procesa información sensible.
- Acceso físico a las áreas sensibles.
- Cambios en el personal.
- Informes completos de los intentos de intrusión física en las infraestructuras que dan soporte al sistema de certificación.

9.4.2. Frecuencia del procesamiento del registro

Los registros de auditoría se procesan y revisan una vez al mes con el fin de buscar actividades sospechosas o no habituales, y los eventos auditables significativos generan avisos automáticos para realizar una auditoría. Los registros implementan medidas que aseguran la integridad de los datos.

9.4.3. Periodo de conservación del registro de auditorías

El registro de auditorías se conserva por un periodo de diez (10) años de acuerdo a la normativa aplicable.

9.4.4. Protección del registro de auditoría

Los archivos del registro de auditorías se encuentran protegidos en su acceso para Administradores de la ER tanto para la lectura como para la escritura.

La ER no destruye ningún archivo de auditoría sin que medie autorización expresa de INDECOPI, siempre y cuando haya transcurrido un periodo mínimo de 10 años.

9.4.5. Procedimiento de copia de seguridad del registro de auditorías

De manera mensual se realiza una copia de seguridad del registro de auditorías, la cual se archivar fuera de las instalaciones de la ER.

9.4.6. Sistema de realización de auditoría (Interna vs Externa)

La Entidad de Registro realiza auditorías internas anualmente. Con igual periodicidad se realizan auditorías externas con evaluación técnica.

9.4.7. Notificación al titular que causa un evento

La ER notifica a los titulares y suscriptores de certificados de eventos que puedan afectar la confianza sobre los servicios de certificación de la ER.

9.4.8. Valoración de vulnerabilidad

La valoración de vulnerabilidades se realiza de acuerdo a la Política de Seguridad de la EC.

9.5. Archivo de registro

9.5.1. Tipos de eventos registrados

Dentro de los archivos de registro se mantienen los datos de los suscriptores y titulares, los contratos y documentos que dan constancia de cada solicitud realizada en la ER, las claves públicas de dicha entidad y el registro de auditorías.

9.5.2. Periodo de conservación del archivo

El periodo de conservación de los archivos es de diez (10) años, así como de las aplicaciones requeridas para su acceso.

9.5.3. Protección del archivo

La protección de los archivos se realiza de acuerdo a lo previsto en la Política de Seguridad de la ER.

9.5.4. Procedimientos para copia de seguridad del archivo

La ER gestiona copias de respaldo de la información y software esencial, con el fin de mantener la integridad y disponibilidad de los servicios de procesamiento de información y comunicaciones, se deben realizar copias de respaldo de la información y software esencial.

9.5.5. Requisitos para los archivos de sellado de tiempo

Los datos archivados contienen la fecha y hora, y se encuentran firmados digitalmente, debidamente secuenciados para generar evidencias de su cronología.

9.5.6. Sistema de recolección del archivo (Interna o Externa)

Los archivos se mantienen por duplicado, incluyendo una copia fuera de las instalaciones de la ER.

9.5.7. Procedimiento para obtener y verificar la información del archivo

Los procedimientos para la obtención y verificación de la información del archivo deben encontrarse de conformidad con los requisitos de confidencialidad y privacidad respetan la normativa de privacidad aplicable.

9.6. Recuperación frente al compromiso y desastre

Se establece un plan de contingencias que permita el restablecimiento y mantenimiento de las operaciones de la ER. Este plan debe contemplar las acciones a realizar, los recursos a utilizar y el personal a emplear en el caso de producirse un acontecimiento intencionado o accidental que inutilice o degrade los recursos y los servicios de certificación.

Dicho plan debe asegurar que los aspectos básicos del negocio, tales como servicios de validación o revocación, puedan ser reasumidos dentro de un plazo máximo de 24 horas, el cual constituye el plazo máximo para la emisión de las listas de revocación de certificados. Los planes deben ser evaluados por lo menos una vez durante el periodo de cada auditoría o evaluación de compatibilidad y los resultados deben ser puestos a disposición de los auditores de compatibilidad o asesores, conjuntamente con la información respecto a las acciones correctivas que pudieran ser necesarias.

9.6.1. Procedimiento de manejo de incidentes y compromisos

La ER establece los procedimientos en esta materia a través de su plan de contingencia.

9.6.2. Adulteración de los recursos computacionales, software y/o datos

El plan debe identificar fuentes alternativas de recursos computacionales, software y datos, las cuales deben ser empleadas en los casos de adulteraciones o fallas en los mismos.

En el caso que la adulteración se refiera al compromiso real o potencial de las claves privadas que pudiera generar su inoperatividad, debe tomarse en consideración la posibilidad de realizar un proceso de reemisión.

9.6.3. Procedimientos en caso de compromiso de la clave privada de la entidad

En el caso de compromiso de la clave privada de un empleado que cumpla un rol de confianza, el certificado deberá ser revocado y se deberá solicitar la emisión de un nuevo certificado.

9.7. Finalización de la EC o ER

Ante la finalización de la ER, BIT4ID informará al INDECOPI, a los suscriptores, titulares y los terceros que confían sobre el cese de sus operaciones con al menos treinta (30) días calendario de anticipación al cese efectivo.

Se transferirán al INDECOPI o bien a otra entidad que éste designe, todos los datos e informaciones necesarias para la continuación de las operaciones por de la Entidad de Registro. En el supuesto de una operación de transferencia de titularidad, se asegurará que la nueva entidad cumple con los requisitos de acreditación de la AAC.

Cuando la EC vinculada finalice o transfiera sus operaciones, se advertirá a todos los suscriptores y terceros que confían, respecto de los cambios y todo tipo de condiciones asociadas a la continuidad del uso de los certificados emitidos, todo ello mediante comunicado publicado en la siguiente dirección: www.uanataca.com/pe.

10. CONTROLES DE SEGURIDAD TECNICA

10.1. Generación e instalación del par de claves

10.1.1. Generación del par de claves

La generación de claves de los usuarios finales se realiza siempre, debe ser realizada utilizando procedimientos de generación de claves compatibles con el estándar FIPS 140-2 o Common Criteria EAL4+ como mínimo. Las claves pueden ser generadas por los propios suscriptores o por la ER de BIT4ID.

10.1.2. Entrega al suscriptor de la clave privada

La ER de BIT4ID en los casos en que genera el par de claves en presencia del usuario hace entrega de los medios al mismo para garantizar el control exclusivo de las mismas.
En aquellos casos en que las claves son generadas en presencia del usuario, la ER genera las claves, y a través de un canal seguro (email, sms, tarjeta de número secreto o similar), transmite directamente las credenciales de uso al titular, para asegurar el control exclusivo de las claves.

10.1.3. Entrega de la clave pública para el emisor de un certificado

Cuando el suscriptor genera su propio par de claves o par de claves del titular, las claves públicas correspondientes son entregadas al emisor del certificado de manera tal que se asegura la autenticidad de dicho suscriptor.

10.2. Controles de ingeniería para protección de la clave privada y módulo criptográfico

10.2.1. Estándares y controles para el módulo criptográfico

Los módulos criptográficos usados por la ER de BIT4ID o eventuales Proveedores de servicios de repositorio acreditados (si fuesen requeridos) cumplen los requerimientos de la norma FIPS 140-2 nivel de seguridad 2 como mínimo o Common Criteria EAL4+.

Asimismo, se indica al suscriptor que se cambien las credenciales (PIN/PUK) al primer uso del certificado

10.2.2. Depósito de clave privada

No se admite el depósito, almacenamiento o copia de claves privadas de firma y autenticación de los usuarios finales, ni de los módulos hardware que los contienen.

10.2.3. Archivo de la clave privada

La ER no archiva las claves privadas empleadas para la firma y autenticación de los usuarios finales, ni de los archivos electrónicos que los contengan (por ejemplo, los archivos con extensión PFX).

10.2.4. Clasificación del módulo criptográfico

Los módulos criptográficos usados por la ER de BIT4ID cumple los requisitos establecidos o son equivalentes a la norma FIPS 140-2 nivel de seguridad 2 o Common Criteria EAL4+ como mínimo.

Los módulos criptográficos usados por los suscriptores de certificados acreditados por la IOFE cumplen los requisitos establecidos o que son equivalentes a FIPS 140-2 o Common Criteria EAL4+ como mínimo.

10.3. Controles de seguridad informática

La ER de BIT4ID, utiliza la infraestructura técnica y lógica de la EC a la que está vinculada con el fin de proteger tanto los sistemas como toda la información y documentación electrónica que se derive de la prestación de servicios propios de una Entidad de Registro.

A continuación se definen los controles y medios de seguridad definidos por la EC.

10.3.1. Medidas de seguridad informática

Se emplea sistemas fiables para ofrecer sus servicios de certificación. Se 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 aplica 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.

10.3.2. 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.

10.3.3. Evaluación del nivel de seguridad informática

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

10.3.4. 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.

10.4. Controles técnicos del ciclo de vida

La ER de BIT4ID, utiliza la infraestructura técnica y lógica de la EC a la que está vinculada con el fin de proteger tanto los sistemas como toda la información y documentación electrónica que se derive de la prestación de servicios propios de una Entidad de Registro.

A continuación se definen los controles y medios de seguridad definidos por la EC.

10.4.1. 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.

10.4.2. 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.

10.4.2.1.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.

10.4.2.2.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.

10.4.2.3.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.

10.4.2.4.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.

10.4.2.5.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.

11. AUDITORIAS DE COMPATIBILIDAD Y OTRAS EVALUACIONES

La ER de BIT4ID se somete a auditorías de compatibilidad de acuerdo a las previsiones de esta RPS.

11.1. Frecuencia y circunstancias de la evaluación

La ER de BIT4ID se somete una vez al año a auditorías de conformidad respecto del marco de la IOFE, y el resultado de dicha auditoría es publicado por la AAC.

11.2. Identidad/Calificaciones de asesores

El equipo de auditoría que evalúa la conformidad de sus operaciones cuenta con personas con experiencia significativa en tecnologías de la información, seguridad y tecnologías de PKI y criptográficas, aprobadas previamente por INDECOPI.

11.3. Relación del auditor con la entidad auditada

Los auditores o asesores son independientes de la organización de la ER de BIT4ID.

11.4. Elementos cubiertos por la evaluación

La auditoría cubre la implementación de las prácticas de personal, procedimientos y técnicas descritas en este documento. Entre los principales elementos donde se enfoca la auditoría son:

a) Identificación y autenticación.
b) Servicios y/o funciones operacionales.
c) Los controles de seguridad física.
d) Los controles para la ejecución de los procedimientos y los controles de personas que aplican para la ER.

e) Controles de seguridad técnicos.

11.5. Acciones a ser tomadas frente a resultados deficientes

Al detectarse una irregularidad, y dependiendo de la gravedad de la misma, se toman entre otras las siguientes acciones:

a) Indicar las irregularidades, pero permitir que continúen sus operaciones hasta la próxima auditoría programada.
b) Permitir que continúe sus operaciones por un máximo de treinta (30) días naturales pendientes a la corrección de los problemas antes de suspenderlo.
c) Suspender las operaciones.

11.6. Publicación de Resultados

Los resultados de las auditorías o evaluaciones de compatibilidad bajo el marco de la IOFE deben ser publicados como parte de la información de estado, la cual es publicada por INDECOPI.

12. OTRAS MATERIAS DE NEGOCIO Y LEGALES

12.1. Tarifas y reembolso

Las ER de BIT4ID, en convenio con las ECs vinculadas, establecen el monto de sus tarifas para la emisión, re-emisión y en general cualquier otro servicio de la ER, cuales son referenciadas en los contratos de suscriptores. Igualmente se referencian las políticas de reembolso.

Las condiciones económicas (tarifas) y de reembolso se encuentran disponibles para su consulta en la dirección internet www.uanataca.com/pe.

12.2. Responsabilidad financiera

12.2.1. Cobertura de seguro

La ER de BIT4ID cuenta con un seguro de responsabilidad civil contra terceros, que cubre al menos el mínimo establecido por la AAC. La cobertura establece un límite de indemnización de hasta 3.000.000 por reclamación y anualidad.

La cobertura del seguro para las entidades finales y sus condiciones se referencian en los términos y condiciones del servicio de la ER.

12.3. Confidencialidad de la información del negocio

12.3.1. Alcances de la información confidencial

Se mantiene de manera confidencial la siguiente información:

- Material comercialmente reservado de la ER, de los suscriptores de empresa y de las terceros que confían, incluyendo términos contractuales, planes de negocio y propiedad intelectual;
- Información que puede permitir a partes no autorizadas establecer la existencia o naturaleza de las relaciones entre los suscriptores de empresa y los terceros que confían;

- Información que pueda permitir a partes no autorizadas la construcción de un perfil de las actividades de los suscriptores, titulares o terceros que confían.
- Información que mantiene, la cual pudiera perjudicar la normal realización de sus operaciones.
- Los motivos o causales de revocación de un certificado.

12.3.2. Responsabilidad de protección de la información confidencial

La ER de BIT4ID en todo momento asegura el cumplimiento de las disposiciones de confidencialidad como las leyes sobre protección de datos, confidencialidad de la información y propiedad intelectual que les fueren aplicables, tal y como está establecido en el Plan de Privacidad y la Norma Marco sobre Privacidad.

No obstante lo anterior, en cumplimiento con la normativa de aplicación se debe permitir la publicación de e información del estado de los certificados, así como la información en relación a la revocación de un certificado sin revelar la razón de dicha revocación. La publicación se podrá limitar a suscriptores legítimos, titulares o terceros que confían.

12.3.3. Plan de privacidad

La ER de BIT4ID garantiza el cumplimiento de los requisitos previstos en 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. Asimismo cuando proceda y cuando de las operaciones se pueda derivar un impacto en la privacidad de las operaciones, se realizar evaluaciones de impacto sobre los derechos de la privacidad de los usuarios.

En cumplimiento de la misma, BIT4ID creado un Plan de Privacidad.

12.3.4. Información tratada como privada

Se debe mantendrá confidencial la siguiente información:

- Información personal provista por los suscriptores, titulares y terceros que confían que no sea la autorizada para estar contenida en certificados y repositorios;
- Información que pueda permitir a partes no autorizadas establecer la existencia o naturaleza de las relaciones entre suscriptores, titulares y terceros que confían;
- Información que pueda permitir a partes no autorizadas la construcción de un perfil de las actividades de los suscriptores, titulares o terceros que confían.

Se permite expresamente la publicación de información respecto a la revocación o suspensión de un certificado, sin revelar la causal que motivó dicha suspensión o revocación.

12.3.5. Información no considerada privada

Se permite la divulgación de información personal sólo en los casos en que exista consentimiento expreso del individuo cuya información corresponde.

12.3.6. Notificación y consentimiento para el uso de información

Los contratos firmados con su suscriptores referencian el tipo de datos personales que pueden ser recolectados, cómo serán utilizados, protegidos y cómo estos pueden ser revisados/corregidos, las circunstancias bajo las cuales serán divulgados, la manera de desagravios y sanciones para las fallas en el cumplimiento del acuerdo con la parte o partes que utilizan o recolectan dichos datos y el consentimiento necesario para su divulgación. Igual referencia contiene las notificaciones con terceros que confían.

12.3.7. Divulgación realizada con motivo de un proceso judicial o administrativo

La ER de BIT4ID permitirá la revelación de información personal a oficiales encargados del cumplimiento de leyes o como parte de un descubrimiento civil, donde se hace una solicitud de conformidad con la ley aplicable en la jurisdicción en donde la ER se encuentra localizada.

12.3.8. Otras circunstancias para divulgación de información

Los suscriptores, titulares y terceros que confían pueden solicitar la divulgación de la información que han provisto a terceros. Se requiere que la divulgación de la información bajo otras circunstancias se realice solamente de conformidad con la CP u otra documentación relevante y que esto se encuentra de conformidad con la ley aplicable y con la Norma Marco sobre Privacidad.

12.4. Derecho de propiedad intelectual

La ER de BIT4ID mantiene derecho de propiedad sobre todos los registros y demás información necesaria para asegurar la continuidad de los servicios.

12.5. Representaciones y garantías

La ER referencia provisiones de garantía y responsabilidad en relación a errores u omisiones, incluyendo limitaciones y exclusiones, términos, condiciones, incluyéndolas en los contratos con los suscriptores, y haciéndolos disponibles para los terceros que confían.

Los suscriptores y/o titulares están obligados a cumplir las obligaciones establecidas en el CP y CPS de la EC vinculada a la ER de BIT4ID. Estas obligaciones se referenciarán en los contratos respectivos. La ER referencia igualmente las obligaciones de los terceros que confían, especialmente las relativas en su necesidad de verificar el estado de los certificados.

Cualquier otro participante que tenga obligaciones o se le ofrezcan garantías se referenciará específicamente en documento relevante.

12.6. Exención de garantías

La ER de BIT4ID responde por las responsabilidades expresamente presentadas en esta RPS y aquellas no previstas expresamente en este documento pero ordenadas por la legislación vigente.

12.7. Limitación de responsabilidad

La ER de BIT4ID limita su responsabilidad a la emisión y gestión de certificados y de pares de claves de suscriptores suministrados.

12.8. Término y terminación

12.8.1. Término

El periodo de validez máximo de la documentación relativa a la ER es de tres (3) años, de acuerdo a la legislación vigente, y su continuidad está sujeta a la acreditación. La modificación de la documentación estará a las indicaciones de INDECOPI o a través del procedimiento de administración del documento previsto en esta RPS.

12.8.2. Terminación

En caso de terminación, la ER informa a INDECOPI, a los suscriptores, titulares y terceros que confían sobre el cese de sus operaciones con por lo menos treinta (30) días calendario de anticipación.

Los procedimientos respectivos se prevén en documentación relevante.

12.8.3. Cláusulas de divisibilidad, supervivencia, acuerdo íntegro, notificación y fuerza mayor

BIT4ID establece, tanto para el contrato de suscriptor y la presente DPR:

- 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.
- 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.
- En ningún caso BIT4ID responderá por caso fortuito y en caso de fuerza mayor.

12.9. Indemnización

La ER de BIT4ID dispone de una garantía con cobertura suficiente de responsabilidad civil. El referido seguro cubrirá el riesgo de la responsabilidad por los daños y perjuicios que se pudiese ocasionar a terceros como resultado de las actividades, cumpliendo así con lo dispuesto normativa de aplicación.

12.10. Notificaciones y comuicaciones individuales con los participantes

Las EC y ERs deben establecer, en sus contratos de suscriptor y terceros que confían, cláusulas de notificación que regulen los procedimientos por los que las partes se notifiquen hechos mutuamente.

12.11. Enmendaduras

12.11.1. Procedimiento para enmendaduras

INDECOPI revisará los cambios efectuados a las políticas y prácticas documentadas por la ER, antes que estos puedan implementarse. La documentación puede requerir una revisión.

12.11.2. Mecanismos y periodo de notificación

Los cambios en las políticas y prácticas de la ER son notificados a los suscriptores, terceros que confían y otras partes tales como otras infraestructuras que reconocen al mismo o ECs con las que existen acuerdos de certificación cruzada, cuando dichos cambios puedan afectarles.

Cualquier cambio en los términos y condiciones básicas (identificadores de políticas, limitaciones de uso, obligaciones de suscriptor, forma de validación de un certificado, limitaciones a responsabilidad, procedimiento de resolución de disputas, periodo dentro del cual los registros de auditoría serán conservados, sistema legal aplicable y conformidad según el marco de la IOFE) será notificado a los suscriptores y terceros que confían.

Las notificaciones se llevarán a cabo de acuerdo con el caso que trate a través de correos electrónicos, o publicación de notificaciones en la página web de BIT4ID.

12.12. Provisiones sobre resolución de disputas

BIT4ID establece, en el contrato de suscriptor, y en el texto de divulgación o PDS, los procedimientos de mediación y resolución de conflictos aplicables.

12.13. Ley aplicable

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 de acuerdo con la Ley N° 27269 y el Reglamento de Ley de Firmas y Certificados Digitales, aprobado por el D.S. 004-2007-PCM.

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