SERVICIOS AUTO ADMINISTRADOS

Declaración de Prácticas de Certificación de la EC BMCert V1.1

Fecha: 12 de Junio, 2023

El presente documento ha sido elaborado según las recomendaciones de la Guía WEBTRUST PRINCIPLES AND CRITERIA FOR CERTIFICATION AUTHORITIES Version 2.2, la RFC 3647: Marco de Políticas de Certificación y Prácticas de Certificación y la Guía de Acreditación para Entidades de Certificación Digital y Entidades Conexas elaboradas por el INDECOPI

CONTROL DE VERSIONES

Versión	Fecha	Autores	Descripción
1.0	19 de septiembre, 2022	Luis Bays Axell Alvarado	Versión inicial.
1.1	12 de junio, 2023	Luis Bays Eder Guerra	Versión final.

BM Tech

Contenido

1. INTRODUCCION

Este documento hace referencia a Infraestructura de Clave Pública (PKI) Declaración de Prácticas de Certificación (CPS) de BMTECH PERÚ S.A.C. (BMCert) para la Raíz y emisión de los tipos de Entidades Certificadoras ECs (CAs) en modos On-line y Off-line (el "BMCert PKI CPS"). Este documento describe las prácticas internas de la EC BMCert y los procedimientos implicados en la emisión de Certificados digitales por la Raíz de la EC BMCert y las EC subordinadas (designados colectivamente la "EC BMCert"). También resume la operación de los sistemas y la administración de las instalaciones usadas para proporcionar servicios PKI.

1.1. Visión general

De acuerdo al Decreto Supremo 052-2008-PCM "Reglamento de la Ley de Firmas y Certificados Digitales" aprobado el 19 de julio del 2008 y sus modificaciones; y al amparo de la Ley N° 27269 "Ley de Firmas y Certificados Digitales", la EC BMCert ha implementado una Infraestructura de Clave Pública (PKI). La PKI consiste de una EC Raíz auto firmada, una EC on-line subordinada (BMCert Issuing CA) y de ser el caso ECs off-line, los repositorios, las entidades de registro, las agencias de registro y los suscriptores asociados a estas Entidades Certificadoras (ECs). La EC Raíz auto-firmada actúa como la EC (BMCert Root CA) principal para la certificación cruzada con otras ECs para lograr la interoperabilidad con otra entidad PKI.

1.2. Nombre e identificación del documento

Nombre del documento	Declaración de Prácticas de Certificación de la EC BMCert
OID	1.3.6.1.4.1.56440.1.1.1
Versión del documento	1
Estado del documento	Versión Final
Fecha de emisión	19 de septiembre 2020
Publicación de la CPS	https://www.bmtech.pe/repositorio/

1.3. Participantes del PKI

Este punto describe la identidad o los tipos de entidades que cumplen los roles de participantes dentro de la PKI, los cuales son:

1.3.1. Entidades de Certificación

La Entidad de Certificación BMCert es la entidad encargada de emitir los certificados para sus suscriptores (Personas Naturales y Jurídicas) según los requerimientos de la

Autoridad Administrativa Competente.

La EC BMCert está encargada de la emisión y revocación de certificados digitales de: Personas Naturales, Personas Jurídicas y de Agentes Automatizados.

La EC BMCert recepciona a través de un medio seguro, con las debidas validaciones de identidad por parte de la ER, las autorizaciones para la emisión y revocación de certificados digitales.

Para el caso de esta PKI, la EC BMCert dispone de dos Entidades de Certificación:

- BMCERT Root CA: Entidad Certificadora raíz, la cual se utiliza únicamente para emitir certificados de Entidad Certificadora Intermediaria y emitir su respectiva CRL, esta Entidad Certificadora se mantiene fuera de línea salvo cuando se requiera.
- BMCERT Issuing CA: Entidad Certificadora intermediaria, la cual se utiliza para emitir los certificados de Entidad Final y su respectiva CRL.

1.3.2. Entidades de Registro

La EC BMCert tiene convenio y vínculo con las siguientes Entidades de Registro:

- ER ABC IDENTIDAD DIGITAL S.A.C.
- ER IOFE S.A.C.

Asimismo, puede proveer sus servicios a través de cualquier ER acreditada.

1.3.3. Suscriptores

Según lo indicado por la AAC, el 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 mensaje de datos firmado digitalmente utilizando su clave privada.

El Titular es la persona natural o jurídica a quien se le atribuye de manera exclusiva un certificado digital y, por tanto, actúa como responsable del mismo, con conocimiento y plena aceptación de los derechos y deberes establecidos y publicados en la CPS.

En el caso que el titular del certificado sea una persona natural, sobre la misma recaerá la responsabilidad de suscriptor.

En el caso que una persona jurídica sea el titular de un certificado, 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 cual deberá ser dueña del agente automatizado. La atribución de responsabilidad de suscriptor, para tales efectos, corresponde al representante legal, que en nombre de la persona jurídica solicita el certificado digital.

1.3.4. Partes o terceros que confían

Los terceros que confían son aquellas personas naturales o jurídicas (diferentes al titular o suscriptor del certificado digital), equipos, servicios, software o cualquier otro ente que decide aceptar y confiar en un certificado digital emitido por la EC BMCert, y actúa basado en la confianza sobre la validez de un certificado digital y/o verifica la firma digital en la que se utiliza dicho documento.

1.3.5. Otros participantes

Otros participantes como autoridades de fabricación de certificados, proveedores de servicios de repositorio y otras entidades que prestan servicios relacionados con el PKI.

1.4. Uso de certificados

1.4.1. Usos apropiados del certificado

Los certificados digitales emitidos por la EC BMCert tendrán como finalidad lo siguiente:

Certificado de Autenticación y Firma: La inclusión de ambos Usos de Clave proporciona las siguientes garantías:

a) Autenticidad de origen

El titular o suscriptor podrá acreditar su identidad frente a cualquiera, demostrando la posesión y el acceso a la clave privada asociada a la clave pública que se incluye en el certificado que acredita su identidad.

b) No repudio de origen

Esta característica se obtiene mediante la firma digital realizada según el articulo 2 de la ley de firmas y certificados digitales, el no repudio hace referencia a la vinculación de un individuo (o institución) con el documento electrónico, de tal manera que no puede negar su vinculación con él, ni reclamar supuestas modificaciones de tal documento.

c) Integridad

Por medio de la firma digital se puede garantizar que un documento electrónico no ha sido alterado desde la transmisión por el emisor hasta su recepción por el destinatario.

1.4.2. Usos prohibidos del certificado

El certificado no se puede usar para fines o aplicaciones no contemplados en el numeral 1.4.1 y las no contempladas en:

- Ley N° 27269 “Ley de Firmas y Certificados Digitales” y Decreto Supremo 070-2011-PCM.
- D.S. 052-2008-PCM “Reglamento de la Ley de Firmas y Certificados Digitales” y normas complementarias.

- Disposiciones de la AAC.
- Declaración de Prácticas y Políticas de Certificación de la EC BMCert.

1.5. Administración de políticas

1.5.1. Organización que administra el documento

La organización encargada de la administración (elaboración, registro, mantenimiento y actualización) de este documento es:

Nombre: BMTech Peru S.A.C.

Dirección de correo: ccom@bmtech.pe

Dirección: Av. Juan de Aliaga, 457, Piso 15, Magdalena del Mar, Lima, Lima, Peru

Teléfono: 01 2461991

1.5.2. Persona de contacto

Nombre: Luis Bays

Dirección de correo: luis@bmtech.pe

Dirección: Av. Juan de Aliaga, 457, Piso 15, Magdalena del Mar, Lima, Lima, Peru

Teléfono: 01 2461991

1.5.3. Persona que determina la idoneidad de la CPS con las políticas

El INDECOPI es la Autoridad Administrativa Competente - AAC, responsable de acreditar y determina si una Entidad de Certificación está dentro de la Infraestructura Oficial de Firma Electrónica (IOFE), asimismo, es quien aprueba la presente Declaración de Prácticas y Políticas de Certificación durante el proceso de acreditación.

1.5.4. Procedimientos de aprobación de la CPS

La AAC decidirá la aprobación de la CPS de la EC mediante los procedimientos establecidos en la "Guía de Acreditación para Entidades de Certificación Digital – EC".

1.6. Definiciones y abreviaturas

1.6.1. Definiciones

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.

Aplicabilidad o propósito de un certificado: se refiere al rango de aplicaciones en las que se puede utilizar un certificado digital dentro de una comunidad. Este rango puede dividirse en tres partes: (a) Aplicaciones libres, destinadas a miembros comunes de una comunidad. (b) Aplicaciones restringidas a un grupo selecto dentro de la comunidad. (c) Aplicaciones prohibidas para cualquier miembro de la comunidad.

Archivo: Es el conjunto organizado de documentos producidos o recibidos por una entidad en el ejercicio de las funciones propias de su fin, y que están destinados al servicio.

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): Según el estado peruano, es el organismo público responsable de acreditar a los Prestadores de Servicios de Certificación, 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.

Criptografía Asimétrica: Es la rama de las matemáticas aplicadas que se ocupa de transformar documentos electrónicos en formas aparentemente ininteligibles y devolverlas a su forma original, las cuales se basan en el empleo de funciones algorítmicas para generar dos "claves" diferentes, pero matemáticamente relacionadas entre sí. Una de esas claves se utiliza para crear una firma numérica o transformar datos en una forma aparentemente ininteligible (clave privada), y la otra para verificar una firma numérica o devolver el documento electrónico a su forma original (clave pública). Las claves están

matemáticamente relacionadas, de tal modo que cualquiera de ellas implica la existencia de la otra, pero la posibilidad de acceder a la clave privada a partir de la pública es técnicamente ínfima.

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.

Depósito o Repositorio de Certificados: Es el sistema de almacenamiento y recuperación de certificados, así como de la información relativa a éstos, disponible por medios telemáticos.

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.

Entidad final o usuario final: suscriptor o titular de un certificado digital.

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.

Hardware: es un neologismo proveniente del inglés, definido por la RAE como el conjunto de los componentes que integran la parte material de una computadora; sin embargo, es utilizado en una forma más amplia, generalmente para describir componentes físicos de una tecnología.

Identificador de objeto OID: Es una cadena de números, formalmente definida usando el estándar ASN.1 (ITU-T Rec. X.660 | ISO/IEC 9834 series), que identifica de forma única a un objeto. En el caso de la certificación digital, los OIDs se utilizan para identificar a los distintos objetos en los que ésta se enmarca (por ejemplo, componentes de los Nombres Diferenciados, CPSs, etc.). Referencia: http://www.oid-info.com/index.htm.

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).

Integridad: característica que indica que un mensaje de datos o un documento electrónico no ha sido alterado desde la transmisión por el iniciador hasta su recepción por el destinatario.

Lista de Certificados Digitales Revocados (CRL): es aquella en la que se deberán incorporar todos los certificados revocados por la entidad de certificación de acuerdo con lo establecido en el Reglamento de la Ley de Firmas y Certificados Digitales.

No repudio: Es la imposibilidad para una persona de desdecirse de sus actos cuando ha plasmado su voluntad en un documento y lo ha firmado en forma manuscrita o digitalmente con un certificado emitido por una Entidad de Certificación acreditada en cooperación de una Entidad de Registro o Verificación acreditada, salvo que la misma entidad tenga ambas calidades, empleando un software de firmas digitales acreditado, y siempre que cumpla con lo previsto en la legislación civil. En el ámbito del artículo 2º de la Ley de Firmas y Certificados Digitales, el no repudio hace referencia a la vinculación de un individuo (o institución) con el documento electrónico, de tal manera que no puede negar su vinculación con él ni reclamar supuestas modificaciones de tal documento (falsificación).

Nombre Diferenciado X.501: es un sistema estándar diseñado para consignar en el campo Sujeto de un certificado digital los datos identificativos del titular del certificado, de manera que éstos se asocien de forma inequívoca con ese titular dentro del conjunto de todos los certificados en vigor que ha emitido la EC. En inglés se denomina "Distinguished Name", DN X.501.

Operadores de registro: Personal de la ER que tiene autorización y responsabilidad para realizar los procesos de verificación de identidad de los solicitantes y transferir las autorizaciones a las Entidades de Certificación.

Par de claves: en un sistema de criptografía asimétrica, comprende una clave privada y su correspondiente clave pública, ambas asociadas matemáticamente.

Política: Orientaciones o directrices que rigen la actuación de una persona o entidad en

un asunto o campo determinado.

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 EC vinculadas.

Práctica: Modo o método que particularmente observa alguien en sus operaciones.

Prácticas de Certificación: prácticas utilizadas para aplicar las directrices de la política establecida en la CP respectiva.

Prácticas específicas de Certificación: prácticas que completan todos los aspectos específicos para un tipo de certificado que no están definidos en la CPS respectiva.

Prácticas de Registro o Verificación: prácticas que establecen las actividades y requerimientos de seguridad y privacidad correspondientes al Sistema de Registro o Verificación de una SVA.

Revocación de Certificados: aquel cambio en el estado del certificado que ocasiona la pérdida de validez del mismo, por alguna circunstancia distinta a la de su caducidad. Cualquier firma digital realizada con un certificado revocado no tendrá validez.

Servicio OCSP (Protocolo del estado en línea del certificado): permite utilizar un protocolo estándar para realizar consultas en línea al servidor de la Autoridad de Certificación sobre el estado de un certificado.

Software: palabra de origen ánglico que hace referencia a todos los componentes intangibles de una computadora, es decir, al conjunto de programas y procedimientos necesarios para hacer posible la realización de una tarea específica. Probablemente la definición más formal de software es la atribuida a la IEEE, en su estándar 729: “la suma total de los programas de cómputo, procedimientos, reglas, documentación y datos asociados que forman parte de las operaciones de un sistema de cómputo”.

Suscriptor: 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. En el caso que una persona jurídica sea el titular de un certificado, 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

cual deberá ser dueña del agente automatizado. La atribución de responsabilidad de suscriptor, para tales efectos, corresponde al representante legal, que en nombre de la persona jurídica solicita el certificado digital.

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 de certificado digital: persona natural o jurídica a quien se le atribuye de manera exclusiva un certificado digital.

Usabilidad: es un término proveniente del inglés "usability", usado para denotar la forma en la que una persona puede emplear una herramienta particular de manera efectiva, eficiente y satisfactoria, en función de lograr una meta específica. A esta idea van asociadas la facilidad de aprendizaje (en la medida en que éste sea lo más amplio y profundo posible), la tasa de errores del sistema y la capacidad del sistema para ser recordado (que no se olviden las funcionalidades ni sus procedimientos).

WebTrust: Certificación otorgada a prestadores de servicios de certificación digital - PSC, específicamente a las Entidades Certificadoras - EC, que de manera consistente cumplen con estándares establecidos por el Instituto Canadiense de Contadores Colegiados (CICA) y el Instituto Americano de Contadores Públicos Colegiados (AICPA). Los estándares mencionados se refieren a áreas como privacidad, seguridad, integridad de las transacciones, disponibilidad, confidencialidad y no repudio.

1.6.2. Abreviaturas

AAC: Autoridad Administrativa Competente.

CP: Políticas de Certificación.

CPS: Declaración de Prácticas de Certificación.

CRL: Lista de Certificados Revocados.

DN: (Distinguished Name) Nombre Distintivo.

EC: Entidad de Certificación.

ER: Entidad de Registro.

FIPS: Federal Information Processing Standards (Estándares Federales de Procesamiento de la Información).

IOFE: Infraestructura Oficial de Firma Electrónica.

OCSP: Online Certificate Status Protocol (Protocolo del estado en línea del certificado).

OID Identificador de Objeto.

PKCS: Public-Key Cryptography Standards.

PKI: Infraestructura de llave pública.

RPS: Declaración de Prácticas de Registro.

2. RESPONSABILIDADES DE PUBLICACIÓN Y REPOSITORIO

2.1. Repositorios

La EC BMCert publica la siguiente información en sus servidores web:

AIA: https://www.bmtech.pe/certs/BMCertChain.p7b

Objetos de la raíz – BMCERT Root CA:

CRL1: http://crl.bmtech.pe/root/BMCERT_ROOT_CA.crl

CRL2: http://crl1.bmtech.pe/root/BMCERT_ROOT_CA.crl

Objetos del intermediario – BMCERT Issuing CA:

CRL1: http://crl.bmtech.pe/issuing/BMCERT_Issuing_CA.crl

CRL2: http://crl1.bmtech.pe/issuing/BMCERT_Issuing_CA.crl

2.2. Publicación de información de certificación

La EC BMCert es responsable de la publicación de la siguiente información, la cual será alojada en el sitio https://www.bmtech.pe/repositorio

- Declaración de Prácticas de Certificación.
- Políticas de Certificación.
- Entidades de Registro vinculadas.

2.3. Hora o frecuencia de publicación

Certificados raíz e intermediario (Cadena de certificación de la EC BMCert): Estos certificados se encuentran publicados por todo el tiempo en que se encuentren vigentes y la EC BMCert se encuentre prestando servicios de Entidad Certificadora. Cuando se requiera reemplazar alguno, se actualizará lo más pronto posible.

Lista de Certificados Revocados (CRL): Para la Entidad Certificadora Raíz, la CRL se actualiza de manera anual. Para la Entidad Certificadora Intermediaria, la CRL se publica con una frecuencia de 4 horas en los dos repositorios. En caso de ser requerido, la EC BMCert puede actualizar una o ambas CRL antes del tiempo estipulado.

Declaración de Prácticas de Certificación (CPS): La CPS se encuentra publicada por todo el tiempo que la EC BMCert se encuentre prestando servicios de Entidad

Certificadora, cuando se realice una modificación, será presentada a la AAC para su debida aprobación, luego de esto será publicada lo más pronto posible. La CPS reemplazada será mantenida en el registro histórico.

2.4. Controles de acceso a repositorios

Los repositorios especificados en los puntos 2.1 y 2.2 cuentan con permisos de lectura de acceso público para que, quien lo requiera, pueda realizar consultas.

La EC BMCert cuenta con controles internos de acceso y procedimientos para evitar la modificación o eliminación no autorizada de información, a fin de garantizar la integridad y autenticidad de esta.

3. IDENTIFICACIÓN Y AUTENTICACIÓN

3.1. Nombres

3.1.1. Tipos de nombres

Todo certificado digital posee un único nombre distinguido (DN, Distinguished Name) conforme al estándar X.501. El uso de los atributos de Asunto (Subject) contenidos en los certificados emitidos por la EC BMCert tiene como base el RFC4519, aplicando algunas variaciones, los cuales se emplean de manera uniforme para cada uno de los perfiles de entidad final conforme se detalla a continuación.

Perfil de Entidad Final	Asunto (Subject)
Persona Natural (OID 1.3.6.1.4.1.56440.3.1)	CN (commonName) = <Nombre completo del Titular> SERIALNUMBER = <Documento de Identidad: Número del documento de Identidad del Titular>(i) E (email) = <Correo electrónico> OU (organizationalUnit) = <Verificado por: Razón Social de la ER solicitante> L (localityName) = <Provincia>(ii) S (stateOrProvinceName) = <Departamento>(ii) C (countryName) = <País>(ii)
Persona Natural con Negocio (OID 1.3.6.1.4.1.56440.3.1.1)	CN (commonName) = <Nombre completo del Titular> SERIALNUMBER = <Documento de Identidad: Número del documento de Identidad del Titular>(i) O (organization) = <Nombre completo del Titular> OU (organizationalUnit) = <RUC: Número de RUC del Titular> E (email) = <Correo electrónico>

	OU (organizationalUnit) = <Verificado por: Razón Social de la ER solicitante> L (localityName) = <Provincia>[ii] S (stateOrProvinceName) = <Departamento>[ii] C (countryName) = <País>[ii]
Persona Natural con Negocio (Agente Automatizado) (OID 1.3.6.1.4.1.56440.3.1.1.1)	CN (commonName) = <Nombre completo del Titular> SERIALNUMBER = <Documento de Identidad: Número del documento de Identidad del Titular>[i] O (organization) = <Nombre completo del Titular> OU (organizationalUnit) = <RUC: Número de RUC del Titular> E (email) = <Correo electrónico> OU (organizationalUnit) = <Verificado por: Razón Social de la ER solicitante> L (localityName) = <Provincia>[ii] S (stateOrProvinceName) = <Departamento>[ii] C (countryName) = <País>[ii]
Persona Natural Profesional (OID 1.3.6.1.4.1.56440.3.1.2)	CN (commonName) = <Nombre completo del Titular> SERIALNUMBER = <Documento de Identidad: Número del documento de Identidad del Titular>[i] G (givenName) = Título Profesional I (initials) = <Siglas del Colegio: Número de colegiatura>[iii] E (email) = <Correo electrónico> OU (organizationalUnit) = <Verificado por: Razón Social de la ER solicitante> L (localityName) = <Provincia>[ii] S (stateOrProvinceName) = <Departamento>[ii] C (countryName) = <País>[ii]
Persona Jurídica (OID 1.3.6.1.4.1.56440.3.2)	CN (commonName) = <Nombre completo del Titular> SERIALNUMBER = <Documento de Identidad: Número del documento de Identidad del Titular>[i] O (organization) = <Razón Social de la Organización> OU (organizationalUnit) = <RUC: Número de RUC de la Organización> T (Title) = Cargo del Titular en la Organización E (email) = <Correo electrónico> OU (organizationalUnit) = <Verificado por: Razón Social

	de la ER solicitante> L (localityName) = <Provincia>[ii] S (stateOrProvinceName) = <Departamento>[ii] C (countryName) = <País>[ii]
Persona Jurídica (Agente Automatizado) (OID 1.3.6.1.4.1.56440.3.2.1)	CN (commonName) = <Nombre completo del Titular> SERIALNUMBER = <Documento de Identidad: Número del documento de Identidad del Titular>[i] O (organization) = <Razón Social de la Organización> OU (organizationalUnit) = <RUC: Número de RUC de la Organización> T (Title) = Cargo del Titular en la Organización E (email) = <Correo electrónico> OU (organizationalUnit) = <Verificado por: Razón Social de la ER solicitante> L (localityName) = <Provincia>[ii] S (stateOrProvinceName) = <Departamento>[ii] C (countryName) = <País>[ii]
Persona Jurídica (Agente Automatizado Anónimo) (OID 1.3.6.1.4.1.56440.3.2.1.1)	CN (commonName) = < Razón Social de la Organización o Seudónimo> SERIALNUMBER = < RUC: Número de RUC de la Organización > O (organization) = <Razón Social de la Organización> OU (organizationalUnit) = <RUC: Número de RUC de la Organización> E (email) = <Correo electrónico> OU (organizationalUnit) = <Verificado por: Razón Social de la ER solicitante> L (localityName) = <Provincia>[ii] S (stateOrProvinceName) = <Departamento>[ii] C (countryName) = <País>[ii]
Persona Jurídica – Trabajador Profesional (OID 1.3.6.1.4.1.56440.3.2.2)	CN (commonName) = <Nombre completo del Titular> SERIALNUMBER = <Documento de Identidad: Número del documento de Identidad del Titular>[i] O (organization) = <Razón Social de la Organización> OU (organizationalUnit) = <RUC: Número de RUC de la Organización> T (Title) = Cargo del Titular en la Organización G (givenName) = Título Profesional

	I (initials) = <Siglas del Colegio: Número de colegiatura> [iii] E (email) = <Correo electrónico> OU (organizationalUnit) = <Verificado por: Razón Social de la ER solicitante> L (localityName) = <Provincia>[ii] S (stateOrProvinceName) = <Departamento>[ii] C (countryName) = <País>[ii]

[i] Los documentos de identidad por defecto son: DNI (Documento Nacional de Identidad), CE (Carné de Extranjería) y Pasaporte. Adicionalmente se pueden utilizar otros documentos de identidad verificados por la ER solicitante.

[ii] Por defecto se tomará la información consignada en el documento de identidad presentado, de no poseerlo se usará el criterio de la ER solicitante.

[ii] Se consideran las siglas referentes a los colegios indicados en la siguiente tabla, también se pueden utilizar otros colegios verificados por la ER solicitante.

Colegios Profesionales	Siglas
Colegio de Abogados de Lima	CAL
Colegio de Abogados de Lima Norte	CALN
Colegio de Abogados del Callao	CAC
Colegio de Notarios de Lima	CNL
Colegio Médico del Perú	CMP
Colegio de Ingenieros del Perú	CIP

3.1.2. Necesidad de que los nombres sean significativos

Los nombres contenidos en el Asunto (Subject) de los certificados emitidos por la EC BMCert, se basan en la nomenclatura especificada en la sección 3.1.1, los cuales son datos comprensibles en lenguaje natural. El uso de los atributos se basa parcialmente en el RFC4519, el uso de algunos atributos ha sido adaptado con la finalidad de consignar en los certificados la información relevante mínima de acuerdo a los identificadores definidos por el Estado Peruano.

Para el caso de certificados que se emitan con fines de prueba, se colocará en el CN (de preferencia al inicio) el texto "SOLO PRUEBAS". Estos certificados carecen de validez legal y solo deberán ser utilizados para fines de pruebas de funcionamiento, software,

integración u homologación, o como muestra cuando la AAC o un auditor designado por esta lo requiera.

3.1.3. Anonimato o seudonimato de los suscriptores

Los certificados emitidos para personas jurídicas correspondientes a agentes automatizados pueden ser anónimos o bajo seudónimo a solicitud del cliente, siempre y cuando sea contemplado por la ER solicitante. En el caso se requiera el anonimato, los atributos donde debería ir la información de la persona física, serán poblados por la información de la persona jurídica. En caso se requiera un seudónimo, este será colocado en el nombre común. Los procedimientos de verificación de seudónimos son determinados por la ER solicitante en su respectiva RPS.

3.1.4. Reglas para interpretar varias formas de nombres

Según lo descrito en la sección 3.1.1, la EC BMCert utiliza el formato de DN como el sujeto del certificado en su caso. Esta forma de nombre será interpretada, en primera instancia, por el estándar X.500, y subsecuentemente de acuerdo con las normas ISO y otras aplicables por Internet.

3.1.5. Unicidad de los nombres

Los nombres se definen de modo inequívoco según lo dispuesto en la sección 3.1.1. El esquema de nombramiento empleado por la EC BMCert se basa sobre identificadores únicos y no debe dar lugar a una "colisión de identificadores".

Sin embargo, si ocurriera una supuesta "colisión de identificadores", la ER responsable de dicha solicitud, resolverá dichas colisiones dentro de su espacio de nombres apropiado.

Si la ER no pudiera resolver satisfactoriamente una "colisión de identificadores", o si la solicitud actual entra en "colisión de identificadores" con una solicitud anterior de una ER distinta, la ER encargada de la solicitud actual someterá la decisión al Oficial de Seguridad de la EC BMCert.

Para evitar conflictos de nombres en certificados correspondientes a personas naturales, la identificación del titular está formada por su nombre y apellidos, más su documento oficial de identidad. En los certificados en los que aparezcan datos de personas jurídicas, la identificación se realiza por medio de su denominación o razón social y su RUC. Además del nombre y apellidos del suscriptor, más su documento oficial de identidad y su cargo o designación temporal.

La duplicidad de nombres se puede dar únicamente cuando los certificados correspondan a perfiles de certificado diferentes, por ejemplo los certificados de Persona Natural con Negocio y los certificados de Persona Jurídica, según si son para Firma Digital sin repudio, o para Firma Digital de Agente Automatizado.

3.1.6. Reconocimiento, autenticación y función de las marcas comerciales.

De conformidad con lo establecido por la AAC, se prohíbe a los solicitantes de certificados de personas jurídicas que incluyan nombres en las solicitudes que puedan suponer infracción de los derechos de terceros. La EC BMCert no podrá volver a asignar un nombre de titular que ya haya sido asignado a un titular diferente.

No es obligación de la EC BMCert, ni de la respectiva Entidad de Registro, verificar si una solicitud de certificado contiene información sujeta a derechos de propiedad intelectual.

En caso la EC BMCert reciba una notificación acerca de que la información de alguno de sus certificados presenta conflicto de nombres, se reserva el derecho de revocar dicho certificado, sin lugar a reclamo por parte del titular.

3.2. Validación de identidad inicial

3.2.1. Método para probar la posesión de clave privada

La EC BMCert envía al titular del certificado un usuario y contraseña en dos correos distintos, los cuales le servirán para autenticarse en el proceso de generación del certificado digital.

La EC BMCert pone a disposición de los titulares de certificados, un aplicativo de generación de certificado, el cual cuenta con dos formas de entregar el certificado digital. El titular es libre de elegir la opción que desee.

a) Generación de la llave privada en el aplicativo: La llave privada se genera dentro del aplicativo, utilizando librerías internas, luego de esto, empleando la respectiva llave pública, se generará la solicitud de certificado en formato PKCS#10 y se enviará a la certificadora, la cual la firmará y devolverá el certificado digital generado. Con ello, el mismo aplicativo procederá a confeccionar el archivo de almacén de certificado en formato PKCS#12 con una contraseña ingresada por el titular, el cual será descargado en el equipo local.

b) Generación de la llave privada fuera del aplicativo: En este caso, el cliente colocará su propio CSR generado por hardware o software (este CSR deberá consignar en el atributo Common Name (CN) el usuario recibido por el titular), el cual será enviado por el aplicativo a la certificadora, la cual firma la llave pública y descarga el certificado junto a la cadena en formato PEM. Según el tipo de certificado, el cliente podrá conservar el certificado en software, o deberá enviar almacenarlo en un dispositivo criptográfico que cumpla con el estándar.

3.2.2. Autenticación de la identidad de la organización

El proceso de autenticación de identidad de las personas jurídicas será realizado según lo establecido en la RPS de la ER solicitante. La EC BMCert deposita su confianza en el proceso de validación establecido por cada ER que ha sido acreditada ante la AAC.

3.2.3. Autenticación de la identidad individual

El proceso de autenticación de identidad de las personas naturales será realizado según lo establecido en la RPS de la ER solicitante. La EC BMCert deposita su confianza en el proceso de validación establecido por cada ER que ha sido acreditada ante la AAC.

3.2.4. Información no verificada del suscriptor

La inclusión o no de la información no verificada del suscriptor será determinada por la RPS de la ER solicitante.

3.2.5. Validación de autoridad

El proceso de validación de autoridad será realizado según lo establecido en la RPS de la ER solicitante. La EC BMCert deposita su confianza en el proceso de validación establecido por cada ER que ha sido acreditada ante la AAC.

3.2.6. Criterios de interoperación

El Oficial de Seguridad de la EC BMCert determinará los criterios de interoperabilidad para las entidades subordinadas (que fueran a utilizar un certificado cruzado) que operan bajo este documento.

3.3. Identificación y autenticación para solicitudes de renovación de claves

3.3.1. Identificación y autenticación para el cambio de clave de rutina

Las solicitudes de reemisión (manteniendo la fecha de expiración del certificado digital) siempre implicarán la revocación del certificado anterior. Esto se detalla en el punto 3.3.2.

Las solicitudes de renovación (donde se emite un nuevo certificado con los mismos datos, solamente modificando la fecha de expiración) serán asumidas como una nueva solicitud a efectos del proceso de identificación y autenticación. La manera de realizar este proceso deberá ser definida en la RPS de la ER solicitante.

3.3.2. Identificación y autenticación para el cambio de clave después de la revocación

Las solicitudes de revocación y reemisión de certificados digitales que sean recibidas en un plazo máximo de 7 días de la fecha de emisión del certificado, podrán ser autenticadas únicamente con un correo electrónico enviado desde la dirección registrada en el certificado en cuestión.

Posteriormente a los 7 días, una solicitud de revocación y reemisión deberá ser

autenticada con alguno de los métodos definidos en la RPS de la ER solicitante.

3.4. Identificación y autenticación para solicitud de revocación

Las solicitudes de revocación pueden ser realizadas a través de la ER que solicitó dicho certificado o directamente a la EC BMCert. Depende quién sea el que solicite a la EC la revocación, se utilizarán distintos mecanismos de autenticación:

a) Solicitud de revocación proveniente de la ER solicitante: La solicitud será autenticada mediante el uso del certificado digital asignado a un Operador de Registro habilitado en dicha ER.

b) Solicitud de revocación proveniente del titular: La solicitud de revocación deberá contener la llave privada correspondiente a la llave pública asociada al certificado a revocar o un mensaje firmado digitalmente con el certificado a revocar. De no ser así, la EC BMCert derivará la solicitud de revocación a la ER que solicitó dicho certificado, para la correspondiente autenticación de la solicitud de revocación.

4. REQUISITOS OPERATIVOS DEL CICLO DE VIDA DEL CERTIFICADO

4.1. Solicitud de certificado

El solicitante que desee gestionar un proceso de solicitud de certificado, deberá entrar en contacto con un representante de alguna de las ER que tengan convenio con EC BMCert y proporcionar la información suficiente para:

- Establecer la autorización del solicitante (representante/apoderado en caso de una persona jurídica) para obtener un certificado digital;
- Establecer y registrar la identidad del solicitante;
- Verificar cualquier papel/rol o información de autorización solicitada para su inclusión en el certificado digital.

4.1.1. Quién puede enviar una solicitud de certificado

A solicitud del interesado, la ER gestionará ante la EC BMCert la emisión de un certificado digital. En tal sentido se encontrarán habilitados para solicitar un certificado digital:

a) Las personas jurídicas, el trámite será realizado por la máxima autoridad administrativa o por el representante legal o una persona designada, quienes deberán contar con las respectivas facultades debidamente acreditas para realizar los trámites ante la ER, convirtiéndose en representantes del titular.
b) Las personas naturales, el trámite será realizado por la propia persona a ser el titular del certificado.

La ER solicitante puede especificar otros escenarios en los que un certificado digital puede ser solicitado. Esto según lo establecido en su respectiva RPS.

4.1.2. Proceso de inscripción y responsabilidades

El proceso de inscripción y la definición de las responsabilidades será realizado según lo establecido en la RPS de la ER solicitante. La EC BMCert deposita su confianza en el proceso de validación establecido por cada ER que ha sido acreditada ante la AAC.

4.2. Procesamiento de la solicitud de certificado

4.2.1. Realización de funciones de identificación y autenticación

La realización de funciones de identificación y autenticación será llevada a cabo según lo establecido en la RPS de la ER solicitante. La EC BMCert deposita su confianza en el proceso de validación establecido por cada ER que ha sido acreditada ante la AAC.

4.2.2. Aprobación o rechazo de solicitudes de certificado

El solicitante que desee gestionar un proceso de solicitud de certificado, deberá apersonarse a una oficina de la ER que cuente con un convenio con la EC BMCert y se encuentre debidamente acreditada. El solicitante debe entregar la información solicitada por la ER y asume la responsabilidad por la veracidad y exactitud de la información proporcionada, sin perjuicio de la respectiva comprobación por parte de la ER.

En caso que una solicitud sea aprobada por una ER con la cual se celebró un convenio, dicha entidad debe realizar lo siguiente:

- Comunicar a la EC BMCert su aprobación para la emisión del certificado. Para ello se han implementado los mecanismos de seguridad necesarios para establecer una comunicación segura con la ER durante el proceso de emisión de certificados y generación del par de claves.
- La ER debe requerir del suscriptor la firma de un contrato de conformidad personal de dichas responsabilidades, así como de conformidad por parte de los titulares, en cuyo nombre actúa el suscriptor.

El contrato antes aludido, deberá contener las obligaciones que deben cumplir los suscriptores y titulares de conformidad con la legislación vigente, para garantizar el efecto legal de las transacciones realizadas empleando un certificado emitido por la EC BMCert, así como las consecuencias de no cumplir con el acuerdo.

El contrato requiere como mínimo al suscriptor y al titular lo siguiente:

- Facilitar a la ER la información completa y adecuada, conforme a los requisitos especificados en su respectiva RPS u otra documentación relevante.
- Manifestar su consentimiento previo a la emisión de un certificado.

- Cumplir las obligaciones que se establecen para el suscriptor y el titular en la CPS de la EC u otro documento relevante y en el contrato del suscriptor.
- Emplear el certificado de acuerdo con lo establecido en la CPS u otro documento relevante de la EC y en el contrato del suscriptor.
- Ser razonablemente diligente en la custodia de su clave privada, con el fin de evitar usos no autorizados, de acuerdo con lo establecido en la CPS de la EC u otro documento relevante y en el contrato del suscriptor.
- Notificar al personal de una ER, sin retrasos injustificables:

a. La pérdida, robo o extravío del dispositivo electrónico de seguridad que almacena su clave privada (computador, token criptográfico o tarjeta inteligente).

b. El compromiso potencial de su clave privada.

c. La pérdida de control sobre su clave privada, debido al compromiso de los datos de activación o por cualquier otra causa.

d. Las inexactitudes o cambios en el contenido del certificado que conozca o pudiera conocer el suscriptor.

- Dejar de utilizar la clave privada, transcurrido el plazo de vigencia del certificado.
- No monitorizar, manipular o realizar actos de ingeniería reversa sobre la implantación técnica de la IOFE, sin permiso previo por escrito de INDECOPI.
- No comprometer intencionadamente la seguridad de la Jerarquía de la IOFE.

4.2.3. Tiempo para procesar las solicitudes de certificado

Una vez autorizada la solicitud por la ER, y comunicada a la EC, ésta última estará en condiciones de emitir el certificado digital de forma inmediata, este tiempo no debe ser mayor a 5 días útiles, a través de un proceso automático.

4.3. Emisión de certificados

4.3.1. Acciones de la EC durante la emisión del certificado

Luego de recibida la solicitud aprobada por la ER, la EC BMCert gestionará la emisión del certificado conforme lo indicado en el punto 3.2.1, dentro de lo cual recibirá una solicitud de firma de certificados (CSR) en formato PKCS#10 y procederá a firmarla junto a la información de identificación provista por la ER. Esto tomará la forma de un certificado digital, el cual será entregado mediante un canal seguro.

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

Inmediatamente después que el certificado digital haya sido emitido, la EC BMCert enviará un correo electrónico a la dirección consignada por el suscriptor, donde se le notificará que su certificado ha sido emitido correctamente.

4.4. Aceptación del certificado

4.4.1. Conducta que constituye la aceptación del certificado

La conducta que constituye la aceptación del certificado digital por parte del titular será determinada según lo establecido en la RPS de la ER solicitante. Siendo generalmente la firma de un Acuerdo de Suscripción y el empleo del certificado digital, los que determinen esta aceptación de manera tácita.

4.4.2. Publicación del certificado por la EC

La EC BMCert publica la relación de los certificados intermediarios emitidos por su entidad raíz tal como se indica en el punto 2.1

La EC BMCert no publica los certificados digitales de entidad final emitidos.

4.4.3. Notificación de la emisión del certificado por parte de la EC a otras entidades

La EC BMCert no informa a terceros sobre los certificados de entidad final que emite. En caso se desee emitir un nuevo certificado intermediario o subsiguiente, se informará debidamente a la AAC.

4.5. Par de claves y uso de certificados

4.5.1. Uso de certificado y clave privada del suscriptor

El alcance previsto de la utilización de la llave privada se especifica a través de las extensiones del certificado, principalmente el Uso de la clave y el Uso mejorado de claves en el certificado asociado.

La EC BMCert exige al suscriptor y al titular, lo siguiente:

- Emplear el certificado de acuerdo con lo establecido en el presente documento y el contrato del suscriptor.
- Ser razonablemente diligente en la custodia de su clave privada, con el fin de evitar usos no autorizados.
- Notificar a la correspondiente ER a través de la cual solicitó su certificado digital, sin retraso injustificable:
  - La pérdida, robo o extravío del dispositivo electrónico de seguridad que almacena su clave privada (computador, token criptográfico o tarjeta inteligente).
  - 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 utilizar la clave privada, transcurrido el plazo de vigencia del certificado

digital.

4.5.2. Uso de certificados y claves públicas por partes que confían

La política de emisión de la EC BMCert especifica restricciones de uso a través de las extensiones de los certificados, como el Uso de la clave y el Uso mejorado de claves. La PKI emite la CRL que especifica el estado actual de todos los certificados no expirados.

La EC BMCert requiere del tercero que confía, como mínimo lo siguiente:

- No monitorizar, manipular o realizar actos de ingeniería reversa sobre la implantación técnica de la AAC.
- No comprometer la seguridad de la Jerarquía de la AAC.
- Aplicar los criterios de verificación adecuados para la validación de un certificado digital durante su uso en las transacciones electrónicas.
- Denunciar cualquier situación en la que se deba cancelar el certificado de un titular, siempre y cuando se tengan pruebas fehacientes del compromiso de la clave privada o de un uso ilegal del manejo de la misma. Por ejemplo, debe denunciar la pérdida, robo o extravío del dispositivo electrónico de seguridad que almacena una clave privada que no le pertenece (computador, token criptográfico o tarjeta inteligente).

4.6. Renovación del certificado

No aplica.

4.6.1. Circunstancia para la renovación del certificado

No aplica.

4.6.2. Quién puede solicitar la renovación

No aplica.

4.6.3. Procesamiento de solicitudes de renovación de certificados

No aplica.

4.6.4. Notificación al suscriptor de la emisión de un nuevo certificado

No aplica.

4.6.5. Conducta que constituye la aceptación de un certificado de renovación

No aplica.

4.6.6. Publicación del certificado de renovación por parte de la EC

No aplica.

4.6.7. Notificación de la emisión del certificado por parte de la EC a otras entidades

No aplica.

4.7. Reemisión del certificado

La EC BMCert, en concordancia por lo dispuesto según la AAC, contempla dentro de sus actividades la reemisión de certificados digitales, la cual se entiende implica una nueva generación de llaves y la solicitud de un nuevo certificado.

La EC comunicará al suscriptor, con una anticipación de al menos 30 días antes de la expiración del certificado, para que pueda renovar a tiempo dicho certificado.

4.7.1. Circunstancias para la reemisión del certificado

Las circunstancias para la reemisión de un certificado digital son las siguientes:

- El certificado actual ha sido revocado por razones de compromiso de la llave privada.
- El certificado actual ha caducado.
- El dispositivo que almacenaba la llave privada y el certificado se ha dañado o extraviado.
- Otras circunstancias definidas por la ER en su respectiva RPS.

4.7.2. Quién puede solicitar la certificación de una nueva clave pública

Sólo el titular de un certificado o un representante legalmente acreditado, puede solicitar a la ER respectiva la re-emisión de su certificado, y la ER la gestionará conforme lo establecido en su RPS.

4.7.3. Procesamiento de solicitudes de reemisión de certificados

El procesamiento de solicitudes de reemisión de certificados será realizado según lo establecido en la RPS de la ER solicitante. La EC BMCert deposita su confianza en el proceso de validación establecido por cada ER que ha sido acreditada ante la AAC.

Como caso especial la ER puede aceptar, como parte de la documentación necesaria para la verificación de identidad, el Acuerdo de Suscriptor firmado digitalmente con el certificado objeto de la reemisión, siempre que el mismo no se encuentre revocado o expirado.

4.7.4. Notificación al suscriptor de la emisión de un nuevo certificado

Este punto se maneja de manera idéntica que el punto 4.3.2.

4.7.5. Conducta que constituye la aceptación de un certificado reemitido

Este punto se maneja de manera idéntica que el punto 4.4.1.

4.7.6. Publicación del certificado reemitido por parte de la EC

Este punto se maneja de manera idéntica que el punto 4.4.2.

4.7.7. Notificación de la emisión del certificado por parte de la EC a otras entidades

Este punto se maneja de manera idéntica que el punto 4.4.3.

4.8. Modificación del certificado

No aplica.

4.8.1. Circunstancia para la modificación del certificado

No aplica.

4.8.2. Quién puede solicitar la modificación del certificado

No aplica.

4.8.3. Procesamiento de solicitudes de modificación de certificados

No aplica.

4.8.4. Notificación al suscriptor de la emisión de un nuevo certificado

No aplica.

4.8.5. Conducta que constituye la aceptación del certificado modificado

No aplica.

4.8.6. Publicación del certificado modificado por la EC

No aplica.

4.8.7. Notificación de la emisión del certificado por parte de la EC a otras entidades

No aplica.

4.9. Revocación y suspensión de certificados

4.9.1. Circunstancias para la revocación

Los certificados serán revocados cuando ocurra una de las siguientes circunstancias:

- Por exposición, puesta en peligro, pérdida, robo, 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 módulo criptográfico que contiene la clave privada se daña, o se bloquea y no es posible su recuperación (o la recuperación implica la exposición

de la misma).

- 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.
- Por iniciativa propia del suscriptor.
- Cuando se descubra que alguno de los datos contenidos en el certificado es incorrecto.
- Por decisión de la legislación respectiva.
- Otras circunstancias que la AAC considere pertinentes.

El titular y/o el suscriptor del certificado están obligados, bajo responsabilidad, a solicitar la revocación al tomar conocimiento de la ocurrencia de alguna de las circunstancias antes mencionadas.

4.9.2. Quién puede solicitar la revocación

Se encontrarán habilitadas para solicitar la revocación de un certificado digital en las circunstancias señaladas en el punto 4.9.1 del presente documento y de acuerdo a lo estipulado por la Ley:

- El titular o suscriptor del certificado.
- La EC BMCert.
- Las Entidades de Registro con las que se tenga convenio.
- Un juez que de acuerdo a 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.

4.9.3. Procedimiento de solicitud de revocación

La EC BMCert acepta los siguientes procedimientos que inician una solicitud de revocación:

- Un mensaje de la ER emisora que se encuentre firmado digitalmente por un Operador de Registro autorizado.
- Un mensaje firmado digitalmente por el suscriptor del certificado.
- Otros procedimientos que la AAC considere pertinentes.

En caso se reciba una solicitud que no siga uno de los procedimientos mencionados, esta será derivada a la ER emisora del certificado en cuestión, la cuál será la encargada de determinar la validez de esta solicitud, y la regresará por el procedimiento designado a la ER.

4.9.4. Período de gracia de la solicitud de revocación

La EC BMCert no es compatible con un período de gracia de la solicitud de revocación de certificados, sino que ésta es tramitada inmediatamente y se procesa según el punto siguiente.

4.9.5. Tiempo dentro del cual EC debe procesar la solicitud de revocación

La EC BMCert revoca certificados tan pronto como sea posible tras la recepción de una solicitud de revocación adecuada. Las solicitudes de revocación se procesan en función del mejor esfuerzo, lo cual será dentro de las 24 horas de la realización de la misma.

4.9.6. Requisito de verificación de revocación para las partes que confían

Una vez realizada la revocación de un certificado por parte de la EC BMCert, ésta publica el estado del certificado en sus repositorios de acuerdo a lo señalado en el ítem 2.3 del presente documento, notificando de esta manera a todo aquel interesado.

4.9.7. Frecuencia de emisión de CRL

Para la Entidad Certificadora Intermediaria, la CRL se publica con una frecuencia de 4 horas en los dos repositorios. En caso de ser requerido, la EC BMCert puede actualizar una o ambas CRL antes del tiempo estipulado.

4.9.8. Latencia máxima para las CRL

Las CRLs cuentan con una latencia máxima de 1 hora, pero generalmente el tiempo entre la emisión y publicación no dura más de 5 minutos. Además, las CRL tienen un tiempo de sobreposición de 15 minutos.

4.9.9. Disponibilidad de verificación de estado / revocación en línea

No aplica.

4.9.10. Requisitos de verificación de revocación en línea

No aplica.

4.9.11. Otras formas de anuncios de revocación disponibles

No aplica.

4.9.12. Requisitos especiales relacionados con el compromiso de la clave

Cuando un certificado de suscriptor es revocado por estar comprometido o se sospecha del compromiso de una clave privada, una CRL se emite inmediatamente después de la notificación, o tan rápidamente como sea posible.

Si se requiere una emisión de CRL de emergencia, la EC puede emitir/publicar la CRL

de inmediato; Sin embargo no hay garantías de que vaya a ser inmediatamente actualizada por los dispositivos que cuenten con la CRL anterior en caché.

4.9.13. Circunstancias para la suspensión

No aplica.

4.9.14. Quién puede solicitar la suspensión

No aplica.

4.9.15. Procedimiento de solicitud de suspensión

No aplica.

4.9.16. Límites del período de suspensión

No aplica.

4.10. Servicios de estado de certificados

No aplica.

4.10.1. Características operativas

No aplica.

4.10.2. Disponibilidad del servicio

No aplica.

4.10.3. Funciones opcionales

No aplica.

4.11. Fin de la suscripción

La EC BMCert dará por extinguida la validez de un certificado digital en los siguientes casos:

- Caducidad de la vigencia del certificado digital.
- Por revocación del certificado por cualquiera de las circunstancias señaladas en el punto 4.9.1 del presente documento.
- Por fallecimiento del suscriptor o extinción de la persona jurídica que es titular del certificado.

El primer caso es de reconocimiento automático por las aplicaciones que hacen uso de certificados digitales; los otros casos son tratados por la ER, según lo indicado en su correspondiente RPS.

4.12. Custodia y recuperación de claves

La EC BMCert no ofrece servicio de custodia de claves. Ninguna parte externa está autorizada a mantener un fideicomiso de llaves asociadas con Certificados emitidos por la EC BMCert.

4.12.1. Política y prácticas de custodia y recuperación de claves

No aplica.

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

No aplica.

5. CONTROLES DE INSTALACIONES, GESTIÓN Y OPERACIONES

5.1. Controles físicos

Los equipos de la EC BMCert y sus servicios web están en un entorno controlado, tal como se describe en las secciones 5.1.1 a 5.1.8. La EC BMCert establece políticas de seguridad física y ambiental para los sistemas críticos y secundarios, las cuales incluyen el control de acceso físico, control ambiental del sitio donde operan los dispositivos criptográficos, seguridad contra incendios y exposición al agua, corte de suministro eléctrico, acceso no intencionado a medios de almacenamiento y recuperación de desastres. Los controles son implementados a fin de asegurar la continuidad del negocio y el restablecimiento rápido de la cadena de certificación en caso sea necesario.

5.1.1. Ubicación y construcción del sitio

La infraestructura para servicios de la EC BMCert se encuentra dentro de un Datacenter ubicado en Lima, Perú. El edificio está repotenciado y remodelado para Datacenter, el cual es su uso exclusivo. Es Sismo resistente según la norma E.30. Se encuentra certificado como TIER III en Diseño y Construcción y está pendiente la certificación TIER III en Operaciones.

5.1.2. Acceso físico

El acceso físico a las instalaciones de la EC BMCert cuenta con Control de Acceso en todas las salas mediante tarjetas magnéticas o control biométrico.

Los controles y soportes de acceso físico y monitoreo consisten en:

- Base de datos de registro de usuarios autorizados para ingreso y estricto procedimiento de verificación de identidad.
- Completa bitácora de registro de eventos.
- Circuito cerrado de televisión con vista de vigilantes y NOC.
- Sistema BMS para el monitoreo de cada componente de los facilities y del servicio.

- Vigilancia 24x7 en caseta blindada.
- El acceso al rack se encuentra sujeto a la aprobación del gestor de servicio de la EC BMCert y de los administradores del Datacenter, además de requerir los implementos de seguridad, lo cual implica el conocimiento y comunicación constante. Además, las actividades a realizar serán preaprobadas y monitoreadas en su ejecución.

5.1.3. Energía y aire acondicionado

5.1.3.1. Continuidad en el Suministro Eléctrico

- La infraestructura de la EC BMCert cuenta con una configuración redundante N+1 de provisión de energía para la sala de servidores.
- El rack dispone en forma estándar, de dos circuitos de energía independientes, alimentados desde fuentes de energía independientes bus A y bus B, redundantes y respaldadas (UPS y generadores).
- 500 KVA conectado en MT.
- Autonomía de 18 horas con recarga en funcionamiento.
- UPS de alta eficiencia con autonomía de 30 minutos a full carga.
- Monitoreo hasta el circuito

5.1.3.2. Climatización

- Equipos redundantes en configuración N+1 mantienen las salas a temperaturas ideales para la operación de equipos de comunicaciones y servidores. Rango manejado de temperatura entre 18 y 22 Cº son aceptables.
- Sensores de clima y humedad monitorean la mantención de las condiciones ambientales de manera permanente.
- Expansión directa.
- Enfriamiento Continuo.
- Contención de pasillo frío.
- Cada equipo cuenta con ATS.
- Doble ruta para cañerías y control.
- Compresor Inverter, Ventiladores ECF, Control Teamwork.

5.1.4. Exposiciones al agua

El sistema de climatización de la sala de servidores es del tipo expansión directa, no se utilizan chillers ni torres de enfriamiento por agua. No se cuenta con tanque elevado.

El sistema de supresión de incendios es del tipo Agente Limpio – Nove 1230, es dieléctrico, no se utiliza agua a presión ni agua desmineralizada para la supresión.

Las instalaciones se encuentran en una zona de muy bajo riesgo de inundación, los propios equipos de climatización de la sala blanca cuentan con sensores de aniego.

5.1.5. Prevención y protección contra incendios

Las instalaciones de la EC BMCert cuentan con sistemas de detección temprana de incendios con tecnologías de aspiración mediante equipos Vesda, además de sensores de humo y sensores de temperatura.

Se cuenta con un sistema de extinción de incendios por gas inerte NOVEC.

Las puertas existentes en las instalaciones soportan incendios hasta por 3 horas (FM Rated 3).

5.1.6. Almacenamiento multimedia

La EC BMCert mantiene estrictos controles de acceso sobre los medios que contienen información sensible, a fin de que solamente el personal autorizado pueda dispone de ellos. El material archivado se almacena en la instalación de almacenamiento de archivos aprobada por la EC BMCert.

5.1.7. Eliminación de desechos

Los residuos de papel que contienen información sensible se depositan en un contenedor de eliminación cerrado en las instalaciones de la EC BMCert. Cuando el contenedor está lleno, el contenido es procesado a fin de imposibilitar la recuperación de la información, y luego es desechado de manera que no presente impacto para el medio ambiente.

Los medios magnéticos que contienen información sensible en forma electrónica se sobrescriben con el software de seguridad aprobado por la EC BMCert, y luego de ello se dispone del medio para su reutilización o destrucción física, según corresponda.

5.1.8. Copia de seguridad fuera del sitio

LA EC BMCert mantiene una copia de las claves de la EC Raíz e Intermediaria en un almacén separado físicamente, el cual cumple con rigurosos controles físicos. Solo el personal autorizado de la EC BMCert tiene acceso a retirar el material de respaldo.

5.2. Controles de procedimiento

5.2.1. Roles de confianza

El presente documento define los siguientes roles de confianza de la EC BMCert, “rol de confianza” se define como aquel rol cuyas funciones o actividades contraen o implican la gestión de algún riesgo en el manejo, uso o acceso a la información y por lo mismo a la continuidad de las operaciones:

- 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 con las tareas de Certificación e incompatibles con

Sistemas.

- Administrador de Sistemas: responsable del funcionamiento correcto del hardware y software que soportan la plataforma de certificados.
- Administrador de CA: responsable de las acciones a ejecutar con el material criptográfico, la realización de alguna función que implique la activación de las claves privadas de las autoridades de certificación o de cualquiera de sus elementos. Asimismo, es responsable principal de la operación de la plataforma de certificados.
- 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 CA. Además, responsable de otras tareas que le delegue el Administrador de CA respecto a la operación de la plataforma de certificados.
- Operador de Registro: persona responsable de colocar las peticiones de certificación y emitir certificados digitales, al igual que de las otras funciones que competen al ciclo de vida de los certificados.
- 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 arriba indicados 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 necesarias por tarea

Las tareas consideradas como sensibles o críticas siempre serán realizadas por al menos dos personas de confianza. Estas tareas comprenden, entre otras:

- Manipulación del dispositivo de custodia de las claves de EC raíz e intermedia.
- Activación de EC raíz para generación de CRL, emisión de nueva EC intermedia u otras.
- Restauración de las claves privadas de EC raíz e intermedia.

Al finalizar las tareas críticas, se debe verificar que se han desactivado los mecanismos de privilegios elevados que hubieren sido activados para la ejecución de las tareas mencionadas.

5.2.3. Identificación y autenticación para cada rol

Las personas asignadas para cada rol son identificadas por el Auditor Interno que se asegurará que cada persona realiza las funciones 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 tarjetas inteligentes y PINs de activación, usuario y contraseña, certificado digital de administrador y concesión de acceso físico a las instalaciones.

5.2.4. Funciones que requieren separación de funciones

Se procede a detallar las funciones que deberán ser realizadas por diferentes personas, dos o más de estas funciones no podrán ser realizadas por la misma persona.

- Todas las funciones del auditor interno.
- Gestión del ciclo de vida de certificados (a excepción de certificados a ser utilizados con fines de pruebas).
- Operación y administración de la plataforma de certificados.

5.3. Controles de personal

5.3.1. Requisitos de calificaciones, experiencia y autorización

El personal a ocupar roles de confianza en la EC BMCert se selecciona basándose en la lealtad, fiabilidad e integridad. Todos los individuos que ocupan estos roles deben cumplir con los siguientes requisitos:

- Han completado exitosamente un programa de entrenamiento apropiado acorde a las funciones a desempeñar;
- Han demostrado la capacidad de desempeñar sus funciones.
- No han sido previamente relevados de los deberes o responsabilidades de PKI por motivos de negligencia o incumplimiento de sus deberes;
- No han sido condenados por un delito grave;
- No presenta conflicto de intereses con respecto a las funciones que le sean asignadas.

5.3.2. Procedimientos de verificación de antecedentes

Los controles de los antecedentes penales y policiales se llevarán a cabo como parte del proceso de selección del personal a ocupar roles de confianza en la EC BMCert.

Si se cuestiona la confiabilidad de un individuo que desempeña un rol de confianza, el individuo será removido de la posición mientras se investiga el problema. Con base en el resultado de la investigación, el Oficial de Seguridad de BMCert puede reintroducir al individuo en el rol de confianza o sacarlo permanentemente de su rol de confianza.

5.3.3. Requisitos de formación

El personal encargado de tareas de confianza ha sido capacitado de acuerdo al plan de formación e incluye los siguientes contenidos:

- Principios y mecanismos de seguridad de la jerarquía pública de certificación.
- Versiones de hardware y aplicaciones en uso.
- Tareas que debe realizar la persona.
- 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.
- Políticas y procedimientos de seguridad correspondientes.
- La Política General de Certificación, Declaración de Prácticas y Políticas de Certificación, Política de Seguridad, Plan de Privacidad, Política de Privacidad y otra documentación que comprenda sus funciones.
- Marco regulatorio de la prestación de los servicios de certificación digital.

5.3.4. Frecuencia y requisitos de reentrenamiento

La formación del personal se actualiza sobre la marcha para pequeños cambios, y en los casos donde haya cambios sustanciales en los tópicos que comprenden el material de formación, se programan nuevas sesiones de capacitación.

5.3.5. Frecuencia y secuencia de rotación de puestos

No aplica.

5.3.6. Sanciones por acciones no autorizadas

Cualquier persona de la EC BMCert que actúe en violación de las prácticas y procedimientos establecidos en el presente documento, ya sea por negligencia o con mala intención, puede tener su condición y privilegios revocados y puede ser objeto de medidas administrativas y disciplinarias. Dependiendo de la gravedad, también se puede dar una de las siguientes acciones: la eliminación de un rol de confianza, la terminación del empleo y el enjuiciamiento.

5.3.7. Requisitos del contratista independiente

Los terceros 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 bajo su responsabilidad podría, una vez evaluada, dar lugar al cese de la designación.

En el caso de que parte de los servicios de certificación sean operados por un tercero, los controles y previsiones realizadas en esta sección, o en otras partes del presente documento, 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 firmado entre la EC y el tercero, debiendo obligarse los terceros a cumplir con los requerimientos exigidos por la EC BMCert.

5.3.8. Documentación proporcionada al personal

Todo el personal de la EC BMCert que ocupe un rol de confianza tiene acceso a la documentación requerida para permitirles desempeñar eficazmente las funciones de su rol asignado.

La documentación que contenga información confidencial será asegurada apropiadamente cuando no esté en uso. El acceso a la documentación sobre sistemas sensibles específicos se limitará al personal de roles de confianza con una necesidad propia de su rol para la ejecución de sus labores.

5.4. Procedimientos de registro de auditoría

5.4.1. Tipos de eventos registrados

Los eventos de los cuales se guarda registro, según distintas categorías, son los siguientes:

a) Relativos a la gestión del ciclo de vida de las llaves de la EC y los certificados:

- Generación de llaves de la EC
- Instalación manual de llaves criptográficas de EC y su resultado (con la identidad del operador)
- Respaldo de llaves de EC
- Almacenamiento de llaves de EC
- Recuperación de llaves de EC
- Actividades de repositorio de llaves de EC
- Uso de llaves de la EC
- Archivo de llaves de EC
- Retiro de material usado para las llaves del servicio
- Destrucción del certificado de la EC
- Autorización de la operación con las llaves de la EC
- Identidad de las entidades que manejan cualquier material de las llaves (como los componentes de las llaves o las llaves almacenadas en dispositivos portables o media)
- Datos de acceso a los dispositivos o los medios que alojan las llaves
- Compromiso de una clave privada

b) Relativos a la gestión del ciclo de vida de los dispositivos criptográficos:

- Dispositivo del equipo e instalación
- Colocar dentro o remover un dispositivo del almacenamiento
- Activación y uso del dispositivo
- Desinstalación del dispositivo
- Designación de un dispositivo para el servicio y su reparación
- Retiro del dispositivo

c) Eventos sensibles respecto a la seguridad:

- Lectura o escritura de registros o archivos sensibles de seguridad, incluyendo los registros de auditoría
- Acciones tomadas contra los datos sensibles de seguridad
- Cambios de perfiles de seguridad
- Uso de mecanismos de identificación y autenticación, considerando ambos casos exitosos y no exitosos (incluyendo múltiples intentos fallidos de autenticación)
- Fallos de los sistemas, del hardware y otras anomalías
- Acciones tomadas por individuos en Roles de Confianza, operadores computacionales, administradores de sistemas, oficiales de seguridad de sistemas.
- Cambios de la afiliación de una entidad
- Decisiones para saltar procesos y procedimientos de cifrado y autenticación, y
- Acceso a los sistemas de la EC y cualquiera de sus componentes

Además, las ER que deseen establecer un vínculo comercial con la EC BMCert, deben demostrar que realizan el registro de los siguientes eventos:

a) Relativos a la solicitud de certificados:

- El método de identificación aplicado y la información usada para el cumplimiento de los requerimientos del suscriptor
- Registro de la data, números o combinación única de identificación o documentos de identificación
- Locación de almacenamiento de las copias de los documentos de identificación y las solicitudes
- Identidad de la entidad que acepta las solicitudes
- Método usado para validar documentos de identificación
- Nombre de la EC que recibe y de la ER que solicita
- Aceptación del suscriptor del Acuerdo del Suscriptor
- El consentimiento para permitir a la EC o ER guardar registros de datos personales, pasar esta información a terceras partes especificadas, y publicación de certificados.

b) Relativos a la gestión del ciclo de vida de los certificados (en este caso, la EC también

registra los eventos de su competencia):

- Recepción de solicitudes de certificados – incluyendo solicitudes iniciales de certificados y solicitudes de re-emisión
- Cambio de afiliación de una entidad
- Generación de certificados
- Distribución de la clave pública de la EC
- Solicitudes de revocación de certificados
- Revocación de certificados
- Solicitudes de suspensión de certificados (si se brinda el servicio)
- Suspensión y reactivación de certificados

Los registros de eventos incluyen como mínimo los siguientes elementos:

- Fecha y hora de la entrada
- Número de serie o secuencia
- Tipo de entrada (según acción realizada)
- Fuente de la entrada
- Identidad de la entidad que realiza la entrada

Todos los eventos son registrados de manera exacta y apropiada.

Los registros de auditoría no registran de ninguna manera llaves privadas.

Los relojes de los sistemas computacionales son sincronizados con una exactitud y la fuente de tiempo confiable.

5.4.2. Registro de frecuencia de procesamiento

Los registros de auditoría son revisados por infracciones de políticas u otros eventos significativos por lo menos una vez al mes. Tales revisiones implican verificar que el registro no ha sido manipulado. Cuando se realizan las revisiones, se extraen y revisan los eventos de un mes entero y se prepara un resumen del registro de auditoría que contiene descripciones detalladas de las advertencias, alarmas y otras irregularidades del registro de auditoría.

5.4.3. Período de conservación del registro de auditoría

En cumplimiento de lo establecido por la AAC, la conservación de los registros de auditoría señalados en el ítem 5.4.1. será como mínimo por un periodo de diez (10) años.

5.4.4. Protección del registro de auditoría

Los registros de auditoría solo pueden ser consultados por el Auditor Interno, cuyo perfil de acceso al sistema de la EC es el único que contiene privilegios de lectura de los registros de auditoría.

Los registros de auditoría no pueden ser modificados ni eliminados por medio del sistema de la EC. Esto puede ser realizado únicamente por el Administrador de Sistemas, que es quien posee acceso a la Base de Datos del sistema de la EC.

El Administrador de Sistemas no está autorizado, bajo ninguna circunstancia, a modificar los registros de auditoría.

El Administrador de Sistemas podrá vaciar completamente la tabla de registros de auditoría, únicamente en el caso en que los datos de dicha tabla hayan sido previamente respaldados y almacenados en un medio seguro. No se deberá realizar un borrado selectivo de registros de auditoría.

5.4.5. Procedimientos de copia de seguridad del registro de auditoría

Los registros de auditoría que se encuentran en el sistema de la EC son respaldados de manera automatizada con una frecuencia diaria.

5.4.6. Sistema de recopilación de auditorías (interno o externo)

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

5.4.7. Notificación al sujeto causante del evento

Cuando el sistema de recopilación de auditoría registra un evento, no es obligatorio enviar una notificación al individuo, organización, dispositivo o solicitud que lo provocó.

5.4.8. Evaluaciones de vulnerabilidad

El análisis de vulnerabilidades queda cubierto por los procesos de auditoría de seguimiento que realiza la AAC anualmente.

Se realizan rutinas de revisión de los registros de auditoría a fin de localizar inconsistencias.

Cualquier problema reportado es corregido y registrado por el Oficial de Seguridad de la EC BMCert.

5.5. Archivo de registros

5.5.1. Tipos de registros archivados

La EC BMCert archiva la siguiente información:

- Todos los datos de auditoría recopilados conforme a la Sección 5.4.

- Información de solicitudes de certificados.
- Documentación que respalda las solicitudes de certificados.
- Información del ciclo de vida de certificados
- Registros concernientes a la operación de los servicios de certificación digital.

5.5.2. Periodo de conservación del archivo

La información relativa a los certificados y cualquier información indicada en el apartado 5.5.1 Tipos de eventos archivados, será mantenida por un periodo mínimo de diez (10) años.

5.5.3. Protección del archivo

La EC BMCert protege la información archivada, de tal manera que solo las personas cuyo rol de confianza implique el acceso a dicho contenido antes de su archivado, puedan acceder a estos recursos. La información archivada está protegida contra la visualización, modificación, eliminación u otra alteración no autorizada a través de su almacenamiento dentro de medios resguardados por controles confiables.

Se mantiene una rutina de verificación de los medios a fin de verificar el correcto funcionamiento de los mismos, al mínimo indicio de desperfecto se procederá a migrar los datos a nuevos medios.

También se dispondrá de los recursos necesarios para evitar la obsolescencia del hardware, sistemas operativos y software que impida el acceso a la información archivada.

5.5.4. Procedimientos de respaldo de archivos

Se realiza copias de seguridad de la información archivada con una periodicidad mensual y en el evento en que se incremente la cantidad de información archivada.

5.5.5. Requisitos para el sellado de tiempo de los registros

Para proteger los archivos de registro la EC BMCert realiza una marca de tiempo (Time Stamping) en el instante en que se genera el registro. Los datos archivados consignan la fecha y hora, y la firma digital de la organización según la RFC 3161.

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

Los sistemas de recopilación de archivos de la EC BMCert son internos.

5.5.7. Procedimientos para obtener y verificar información de archivo

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

5.6. Cambio de clave

Con un tiempo de anticipación prudente antes de la expiración de los certificados de EC, se realizará el cambio de llaves, procedimiento que seguirá la misma lógica y tendrá el mismo nivel de seguridad que el efectuado para la emisión de las llaves privadas y sus respectivos certificados de EC por primera vez.

5.7. Compromiso y recuperación ante desastres

5.7.1. Procedimientos de manejo de incidentes y compromisos

La EC BMCert establece los procedimientos a seguir en caso de ocurrir un evento o compromiso real o potencial, indicando la acción que ha de emprenderse al tomarse conocimiento de un incidente.

Estos mecanismos contemplan que, ante la detección de un supuesto incidente o violación de la seguridad de información, deberá ser comunicado a través de canales preestablecidos tan pronto como se haya tomado conocimiento, al Oficial de Seguridad de BMCert para las acciones correspondientes.

El Oficial de Seguridad de BMCert es notificado por correo electrónico inmediatamente en un máximo de 1 hora del descubrimiento del problema (suponiendo que las comunicaciones por correo electrónico en general no se vieron afectadas por la circunstancia que hubiere causado el fallo catastrófico) si la EC BMCert experimenta lo siguiente:

- Sospecha o detección de compromiso en los sistemas de la EC;
- Penetración física o electrónica de los sistemas de la EC; o
- Ataques de negación de servicio exitosos en los componentes de la EC

5.7.2. Los recursos informáticos, el software y / o los datos están dañados

Cuando los recursos informáticos de la EC, software y/o datos están dañados, la EC BMCert, que opera bajo el presente documento, responde de la siguiente manera:

1. Antes de volver a la operación, debe asegurase de que se ha restaurado la integridad del sistema.

2. Si las claves de firma de la EC no se destruyeron, la operación de la EC se restablece restaurando la base de datos desde la copia de seguridad y reinstalando el software.

3. Si se destruyen las claves de firma EC, se vuelve a emitir la clave y el certificado de la EC y se restablece la operación lo más rápidamente posible.

5.7.3. Procedimientos de compromiso de la clave privada de la entidad

En caso una llave de la EC BMCert fuera comprometida de manera real o potencial, ésta

deberá ser inmediatamente revocada, notificándose el hecho en un lapso máximo de 24 horas a la AAC.

Asimismo, se comunicará a las ER para que informe a los suscriptores afectados, que los certificados suministrados con la llave comprometida de la EC, han dejado de ser válidos; estando los usuarios en la facultad de apersonarse a las oficinas de la respectiva ER para solicitar la emisión de un nuevo certificado digital.

5.7.4. Capacidades de continuidad del negocio después de un desastre

La EC BMCert mantiene controles para poder garantizar la continuidad de las operaciones en caso de desastre, según se indica:

Se cuenta con un Plan de Continuidad de Negocio y Recuperación de Desastres, el cual incluye procesos de recuperación para los componentes críticos de los sistemas de la EC. Este plan se prueba de manera anual, y también es evaluado durante el periodo de cada auditoría. Estos resultados están a disposición del Auditor Interno y del auditor designado por la AAC en cada auditoría de seguimiento.

Se cuenta con un local alterno que dispone del equipamiento necesario para reasumir los servicios de revocación y validación de certificados en un plazo máximo de 24 horas. Esto garantiza la continuidad de la recepción de solicitudes de revocación, revocación, emisión de la lista de certificados revocados y publicación de la lista de certificados revocados.

5.8. Terminación de la EC o ER

Antes del cese de actividades, la EC BMCert realizará lo siguiente:

- Poner a disponibilidad de los suscriptores y terceros que confían la información concerniente a la conclusión de sus operaciones.
- Terminar con las autorizaciones de todos los subcontratistas que actúan en nombre de la EC, en el proceso de emisión de los certificados digitales.
- Transferir sus obligaciones a una parte confiable para mantener los archivos de los logs de eventos y registros de auditorías necesarios para demostrar la correcta operación de la EC por un periodo razonable.
- Transferir sus obligaciones a una parte confiable para mantener disponible su clave pública o sus certificados a los terceros que confían por un periodo razonable de tiempo.
- Destruir las claves privadas, incluyendo las copias de respaldo, de tal manera que no puedan ser recuperadas.
- Transferir al propio INDECOPI o a otro PSC designado por éste, todos los datos necesarios para la continuación de las operaciones bajo el marco de la IOFE, en particular los certificados raíz y las listas de certificados revocados.

Informar a la AAC, a los suscriptores, titulares y terceros que confían sobre el cese de las operaciones con, por lo menos, treinta (30) días calendario de anticipación.

6. CONTROLES DE SEGURIDAD TÉCNICA

La información contenida en esta sección es relativa a los controles técnicos de seguridad implementados por la EC BMCert, donde se definen las medidas de seguridad tomadas para proteger las claves criptográficas y los datos de activación.

6.1. Generación e instalación de pares de claves

6.1.1. Generación de pares de claves

6.1.1.1. Generación de pares de claves de la EC

Los pares de claves de las entidades de certificación Raíz e Intermediaria han sido creados en módulos de seguridad de hardware (HSM) que cumplen con el estándar FIPS 140-2 nivel 3. El proceso de preparación y generación de las claves ha sido efectuado siguiendo el "Guion de la Ceremonia de Generación de Llaves de la EC (EC BMCert)", cuya ejecución fue registrada en video y captura de pantalla; y se tienen las evidencias de la transparencia del procedimiento y cumplimiento del protocolo. El proceso de generación de las claves ha sido realizado dentro del ambiente seguro de las instalaciones del Datacenter donde se encuentra la infraestructura de hardware de la EC BMCert, y ha sido atestiguado por un auditor externo a la EC.

6.1.1.2. Generación de pares de claves de suscriptor

El par de claves de firma para suscriptores de nivel de Seguridad Media se genera utilizando un módulo criptográfico de hardware que se valida conforme a la norma FIPS 140 de nivel de seguridad 1 o superior. El suscriptor únicamente presentará su CSR en formato PKCS#10, el cual servirá de evidencia de que el suscriptor cuenta con la posesión de la clave privada asociada.

6.1.2. Entrega de clave privada al suscriptor

La EC BMCert no hará entrega de claves privadas al suscriptor, el suscriptor deberá generar su propia clave privada utilizando un dispositivo que cumpla con el estándar FIPS 140-2 nivel 1 como mínimo (por ejemplo, un Token de Hardware o una SmartCard).

6.1.3. Entrega de clave pública al emisor del certificado

El suscriptor, utilizando el usuario y contraseña provisto anteriormente, iniciará sesión en el aplicativo de descarga de certificado provisto por la EC BMCert estableciendo una conexión bajo el protocolo TLS, en este, aplicativo el suscriptor colocará su CSR en formato PKCS#10, el cual contiene la clave pública asociada a la clave privada en

posesión del suscriptor.

6.1.4. Entrega de claves públicas de EC a partes confiantes

Las claves públicas de la EC Raíz e Intermediaria se encuentran publicadas en el sitio web, el cual cuenta con Autenticación del Servidor bajo una conexión segura empleando el protocolo TLS 1.2 o superior. Los terceros que confían pueden acceder al sitio web y descargar los certificados que contienen las claves públicas, de manera individual en formatos PEM y DER, o como cadena completa en formato PKCS#7

6.1.5. Tamaños de clave

Los certificados de la EC Raíz e Intermediaria cuentan con llaves RSA de 4096 bits y algoritmo hash de firma SHA256.

Los certificados emitidos para Entidades Finales utilizan llaves RSA con un tamaño mínimo de 2048 bits y algoritmo hash de firma SHA256.

6.1.6. Generación de parámetros de clave pública y control de calidad

Según el RFC 4055, para certificados con claves RSA el campo Parámetros de clave pública debe contener el valor NULL (05 00). En caso se requiera utilizar certificados de Curva Elíptica (ECC), se generarán los parámetros de clave pública de acuerdo a lo indicado en el RFC 5480.

6.1.7. Propósitos de uso de claves

Los certificados de EC Raíz e Intermediaria cuentan con los Usos de Clave: Firma de Certificados (Certificate Signing) y Firma de CRL (CRL Signing).

Las claves de la EC Raíz, serán utilizadas únicamente para firmar nuevas entidades emisoras (intermediarias) y su respectiva CRL de manera anual.

Las claves de la EC Intermediaria serán utilizadas para firmar los certificados de Entidad Final y su respectiva CRL.

6.2. Protección de clave privada y controles de ingeniería del módulo criptográfico

6.2.1. Estándares y controles del módulo criptográfico

La AAC indica que el módulo criptográfico donde se generan las llaves de EC debe cumplir con el estándar FIPS 140-2 nivel 3 o superior, lo cual es conforme respecto a los módulos criptográficos que conforman la infraestructura de la EC BMCert.

Sobre las llaves del suscriptor, la norma impuesta por la AAC para Seguridad Media, es que el módulo criptográfico utilizado por el suscriptor debe cumplir con el estándar FIPS 140-2 nivel 1 como mínimo.

6.2.2. Clave privada (n de m) control de varias personas

Estipulado en el documento: Guion de la Ceremonia de Generación de Llaves de la EC (EC BMCert).

6.2.3. Depósito de clave privada

Acerca de las claves de la EC, la información se encuentra estipulada en el documento: Guion de la Ceremonia de Generación de Llaves de la EC (EC BMCert).

La EC BMCert no admite el depósito, almacenamiento o copia de claves privadas de los usuarios finales, ni de los módulos de hardware que los contienen. Ninguna parte externa está autorizada a mantener un fideicomiso de claves asociadas con los certificados expedidos por la EC BMCert.

6.2.4. Copia de seguridad de la clave privada

Estipulado en el documento: Guion de la Ceremonia de Generación de Llaves de la EC (EC BMCert).

6.2.5. Archivo de claves privadas

Cuando los certificados Raíz o Intermediario de la EC BMCert expiren, sus claves privadas asociadas serán archivadas por un periodo mínimo de 10 años con el mismo nivel de seguridad que las claves en producción.

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

Las claves privadas de la EC BMCert nunca son transferidas fuera del Security World donde han sido generadas.

6.2.7. Almacenamiento de clave privada en módulo criptográfico

El almacenamiento de la clave privada cumple con el estándar FIPS 140-2 nivel 3. Mayor detalle se encuentra en el documento: Guion de la Ceremonia de Generación de Llaves de la EC (EC BMCert).

6.2.8. Método de activación de la clave privada

Los procedimientos de activación de las claves privadas de la EC BMCert se realizan de igual manera a lo estipulado en el documento: Guion de la Ceremonia de Generación de Llaves de la EC (EC BMCert).

Los suscriptores con certificados activan su clave privada mediante la autenticación en su módulo criptográfico. Los métodos de autenticación incluyen, pero no se limitan a frases/preguntas, PIN o datos biométricos (huella). La entrada de los datos de activación está protegida contra la divulgación (es decir, los datos no se muestran mientras se introducen).

6.2.9. Método para desactivar la clave privada

Las claves privadas de la EC BMCert son desactivadas cuando se detiene el proceso de precarga de las tarjetas de los operadores (OCS), el apagado del HSM o del servidor. Esto puede ser realizado solamente por el personal autorizado por la EC.

6.2.10. Método de destrucción de la clave privada

Para la eliminación de las claves privadas de la EC BMCert, se debe realizar el borrado de las tarjetas de los operadores (OCS) y la eliminación de los archivos asociados a las tarjetas y llaves dentro del Security World, también se eliminará la copia de respaldo. Este proceso será realizado en una ceremonia la cual contará con las mismas medidas de seguridad que la ceremonia de generación de llaves.

Las claves privadas del suscriptor deberán ser borradas directamente desde el módulo criptográfico donde se encuentren almacenadas.

6.2.11. Clasificación del módulo criptográfico

Los módulos criptográficos usados por la EC BMCert cumplen los requerimientos de FIPS 140-2 nivel 3, tanto en hardware como en firmware. Igualmente, el Security World ha sido creado indicando que se debe cumplir de manera estricta el referido estándar.

6.3. Otros aspectos de la gestión de pares de claves

6.3.1. Archivo de claves públicas

La EC BMCert mantiene un archivo de todas las claves públicas contenidas en los certificados que emite.

6.3.2. Períodos operativos del certificado y períodos de uso de pares de claves

Los certificados digitales emitidos por la EC BMCert tendrán una vigencia máxima de 3 años. Los pares de claves pueden ser utilizados solo durante este tiempo. Luego de ello, no podrán ser utilizados debido a que la EC BMCert no emitirá un certificado con la misma llave pública.

6.4. Datos de activación

6.4.1. Generación e instalación de datos de activación

Los datos de activación que son necesarios para acceder a las claves privadas de la EC BMCert consisten en las tarjetas de operador (OCS), un juego de tarjetas para la raíz y otro para la intermediaria. La generación e instalación de los mismos está descrito en el documento: Guion de la Ceremonia de Generación de Llaves de la EC (EC BMCert).

6.4.2. Protección de datos de activación

Cada tarjeta individual OCS está protegida por una contraseña. Las OCS se encuentran almacenados en una bóveda segura, a la cual solo puede acceder el personal autorizado, además que están guardados de tal modo que se evidencien manipulaciones.

6.4.3. Otros aspectos de los datos de activación

Los datos de activación solo serán utilizados en los siguientes eventos:

- Generación de la CRL de la EC Raíz, de manera anual.
- Cuando se vaya a firmar una nueva EC intermediaria.
- En caso de algún fallo que ocasione el desactivado de las llaves de la EC Intermediaria.

La información sobre destrucción de los datos de activación se describe en el punto 6.2.10.

6.5. Controles de seguridad informática

6.5.1. Requisitos técnicos específicos de seguridad informática

La EC BMCert, servidores y las comunicaciones con la ER cumple los controles establecidos en:

- La norma ISO/IEC 17799 “Information technology – Code of practice for information security management” y la norma ISO/IEC TR13335 “Information technology - Guidelines for the management of IT Security”.
- La norma ISO/IEC 27001:2005 “Information technology - Security techniques - Information security management systems - Requirements”.
- La norma ISO/IEC 15408 “Information technology - Security techniques - Evaluation criteria for IT security”.

Los sistemas operativos cuentan con las siguientes funciones de seguridad habilitadas:

- Control de acceso discrecional;
- Auditoría de seguridad habilitada;
- Acceso restringido a los servicios de la EC; y
- Protector de pantalla con un valor de tiempo de espera no mayor de 10 minutos y la necesidad de volver a autenticar.

El sistema operativo está diseñado y configurado para proporcionar autoprotección y aislamiento del proceso.

6.5.2. Clasificación de seguridad informática

No aplica.

6.6. Controles técnicos del ciclo de vida

6.6.1. Controles de desarrollo del sistema

Como se describe en la Sección 5.4.2 del presente documento, los recursos asignados por el Oficial de Seguridad de BMCert son responsables de revisar los registros de auditoría de la aplicación de la EC periódicamente para asegurar que no se produzcan modificaciones no autorizadas en el software instalado. En el caso de que se detecte una modificación no autorizada, el recurso asignado por el Oficial de Seguridad de BMCert coordina la respuesta del incidente con el personal apropiado.

La sección 5 (y las subsiguientes secciones) anteriores definen las protecciones físicas de seguridad que se han implementado para proporcionar protección a los sistemas de la EC.

Sólo las aplicaciones requeridas por los sistemas de la EC BMCert para el correcto funcionamiento y mantenimiento se instalan en los servidores de aplicaciones de la EC. Las protecciones de seguridad física restringen la posibilidad de que el software malicioso se inserte en el servidor que aloja la aplicación de la EC. Además, según lo determinado por el Oficial de Seguridad de BMCert, las revisiones periódicas del registro de auditoría por un recurso asignado por el Oficial de Seguridad de BMCert se utilizan para supervisar todos los intentos de acceso exitosos y sin éxito realizados a los servidores de la EC.

La EC BMCert y sus Socios Comerciales actúan siguiendo una metodología formal de implementación de software para la instalación y el mantenimiento continuo de los servicios de EC. La metodología formal de gestión del cambio se define en un procedimiento de gestión de cambios documentado. La metodología incluye la creación de documentación de referencia de configuración, seguimiento de cambios, documentación de cambios y clasificación en cuanto a urgencia y complejidad, pruebas de aceptación en un entorno de prueba, revisión por un tablero de control de cambios, implementación del cambio en el entorno de producción de acuerdo con un plan de documentación y actualización del documento de referencias de configuración.

6.6.2. Controles de gestión de seguridad

Como se describe en la Sección 5.4.2 del presente documento un recurso asignado por el Oficial de Seguridad de BMCert es responsable de revisar los registros de auditoría de los servidores de la EC cuando lo determine el Oficial de Seguridad de BMCert para asegurar que no se produzcan modificaciones no autorizadas en el software instalado. En el caso de que se detecte una modificación no autorizada, el recurso asignado por el Oficial de Seguridad de BMCert coordina la respuesta del incidente con el personal apropiado.

6.6.3. Controles de seguridad del ciclo de vida

Los controles de seguridad deben ser revisados como parte de la auditoría o evaluación

de compatibilidad con la ER.

6.7. Controles de seguridad de la red

Las arquitecturas de red BMCert y sus socios de negocios, emplean un enfoque de zona de seguridad de capas múltiples para proporcionar niveles adecuados de seguridad de red para cada componente que comprende el servicio de la EC. Las medidas de protección de límites (por ejemplo, cortafuegos y sensores de detección de intrusos) se implementan en las interfaces de zonas de seguridad y se han implementado para denegar todos los servicios necesarios, excepto los necesarios para los equipos de la EC.

Los firewalls han sido configurados para cuando hay fallas, se detiene todo el tráfico (fail closed). Todos los puertos y servicios de red no utilizados están deshabilitados. Todo el software instalado en los equipos de la EC es necesario para el correcto funcionamiento de esta.

6.8. Sellado de tiempo

No aplica.

7. PERFILES DE CERTIFICADOS, CRL Y OCSP

7.1. Perfil de certificado

Los certificados emitidos por la EC BMCert bajo la presente política siguen los lineamientos del estándar X.509 versión 3 y el RFC3739.

7.1.1. Número (s) de versión

La EC BMCert emite certificados X.509 Versión 3.

7.1.2. Extensiones de certificados

Las extensiones de certificados se encuentran definidas en el documento: Perfiles de Certificados de la EC BMCert, el cual deberá estar a disposición de cualquier tercero autorizado que lo requiera.

7.1.3. Identificadores de objetos de algoritmo

Los Certificados emitidos utilizan el siguiente algoritmo de firma:

Signature Algorithm Identifier	OID
sha256WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}

7.1.4. Formas de nombres

El formato de nombres está de acuerdo a lo recomendado por el estándar X.501, así como

se especifica en el punto 3.1.1 del presente documento.

7.1.5. Restricciones de nombre

Las restricciones de nombre se manejan según lo determinado en la RFC 5280. Además, los nombres contenidos en los certificados emitidos por la EC BMCert permiten el reconocimiento de la personal natural o jurídica para la cual es emitido, salvo el caso en el que se use un seudónimo.

7.1.6. Identificador de objeto de política de certificados

La EC BMCert cuenta con el OID 1.3.6.1.4.1.56440 que fue asignado por la IANA (Autoridad de Números Asignados en Internet), los certificados raíz e intermediario contienen el OID 1.3.6.1.4.1.56440.1.1 el cual hace referencia al presente documento.

7.1.7. Extensión de uso de restricciones de política

No aplica

7.1.8. Sintaxis y semántica de los calificadores de política

No aplica

7.1.9. Procesamiento de semántica para la extensión de políticas de certificados críticas

No aplica

7.2. Perfil CRL

7.2.1. Número (s) de versión

Las CRL emitidas por la EC BMCert son versión 2 (X.509 v2).

7.2.2. Extensiones de entrada de CRL

Las CRL emitidas por la EC BMCert cuentan con las extensiones estándar de las CRL según la RFC 5280.

7.3. Perfil OCSP

La EC BMCert emplea el servicio OCSP según el estándar IETF RFC 6960.

7.3.1. Número (s) de versión

Según el estándar IETF RFC 6960.

7.3.2. Extensiones OCSP

Según el estándar IETF RFC 6960.

8. AUDITORÍA DE CUMPLIMIENTO Y OTRAS EVALUACIONES

8.1. Frecuencia o circunstancias de la evaluación

El cumplimiento de las auditorías de los servicios de la EC se lleva a cabo de acuerdo con el siguiente programa:

- Dentro de los 12 meses del inicio de las operaciones (auditoría de cumplimiento total); y
- Al menos una vez cada 12 meses a partir de entonces.

Todas las personas que realizan roles de confianza de la EC BMCert están sujetos a auditorías periódicas. Estas auditorías se realizarán al menos una vez cada 12 meses, contados a partir de la fecha de nombramiento como de roles de confianza.

En el caso de una auditoría no periódica, el Oficial de Seguridad de la EC BMCert notificará al correspondiente rol de confianza la razón por la que se realiza la auditoría. Dicha notificación se remitirá por escrito y será firmado por el Oficial de Seguridad de BMCert. El Oficial de Seguridad de BMCert mantendrá una copia de cada notificación de auditoría aperiódica.

8.2. Identidad / calificaciones del evaluador

El Oficial de Seguridad de la EC BMCert tiene la responsabilidad de auditar los componentes de la EC y de algunas de las personas que realizan roles de confianza para el PKI de la EC BMCert.

La auditoría de las funciones de la EC puede ser realizada por un recurso interno asignado por el Oficial de Seguridad de EC BMCert o por un equipo auditor externo a ser contratado por el Oficial de Seguridad de la EC BMCert. El auditor debe demostrar la competencia en el campo de las auditorías de cumplimiento y debe estar muy familiarizado con esta CPS y el CP BMCert. El auditor realiza auditorías de cumplimiento, tales como una actividad comercial en curso regular.

8.3. Relación del evaluador con la entidad evaluada

La realización de la auditoría de cumplimiento de la EC es anunciada por el Oficial de Seguridad de BMCert.

En todos los casos, los auditores o asesores que intervienen en las auditorías o evaluaciones de conformidad de la EC BMCert serán independientes y no tendrán ningún tipo de vinculación con la EC BMCert.

8.4. Temas cubiertos por la evaluación

La auditoría de cumplimiento verifica que los controles operacionales y técnicos utilizadas por la EC BMCert para operar los servicios de la EC y todas las personas que realizan los Roles de Confianza con el PKI satisfacen todos los elementos de este CPS.

Entre los principales elementos donde se enfocará 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 EC.
e) Controles de seguridad técnicos.

8.5. Acciones tomadas como resultado de una deficiencia

El Oficial de Seguridad de BMCert ha definido un espectro de acción a seguir en el caso de una deficiencia que se identifica durante la auditoría de cumplimiento. Hay cuatro puntos predefinidos en el espectro, aunque el Oficial de Seguridad de BMCert, trabajando con el Auditor de cumplimiento puede definir otros puntos intermedios adicionales a la situación indicada.

El extremo inferior del espectro comienza con la acción 1 y la gama alta del espectro termina con Acción 4. Los siguientes son los cuatro puntos de acción predefinidos que componen el espectro:

1. Continuar operando como de costumbre

2. Continuar operando, pero dejará de emitir nuevos certificados

3. Suspender temporalmente las operaciones

4. Terminar las operaciones

Si se identifica una deficiencia, el Oficial de Seguridad de BMCert, con el aporte del Compliance Auditor, determinará qué punto del espectro está justificado. En la determinación de la acción que puedan tomar, el Oficial de Seguridad de BMCert debe tener en cuenta la amenaza presentada por la deficiencia, el riesgo que la amenaza podría llevarse a cabo y el impacto si la amenaza se llevó a cabo con éxito. Las sentencias que siguen se proporcionan la guía para ayudar al Oficial de Seguridad de BMCert y el Auditor de cumplimiento para determinar el curso de acción apropiado:

1. Acción 1 que implica que a pesar de que en alguna parte de la Auditoría de Cumplimiento se identificó la deficiencia, la deficiencia no significa una importante amenaza para la integridad del PKI o los certificados que ha emitido, o que el riesgo de que se pudiera llevar a cabo la amenaza.

2. Acción 2 está indicada cuando hay un aumento en el nivel de riesgo o la amenaza a más de la acción 1 que es suficiente para justificar que no sean emitidos nuevos certificados PKI hasta que se resuelva la deficiencia. Las deficiencias en este nivel crean las preocupaciones fundamentales de integridad, disponibilidad o confidencialidad, sin embargo, se han identificado deficiencias importantes que ponen en duda los procesos y los procedimientos adecuados se están siguiendo.

3. Acción 3 se indica cuando hay una deficiencia significativa que plantea una amenaza inmediata o que muestre que la amenaza se podría realizar y cree una situación que seriamente pondría en duda la honradez de los certificados publicados por el PKI.

4. Acción 4 se indica cuando la combinación de la amenaza y el riesgo asociado son suficientes para comprometer la integridad de la PKI e invalidar la fiabilidad de los certificados PKI para su publicación.

Pueden ocurrir los siguientes resultados con respecto a las acciones:

1. Si se toma la acción 1 o 2, el Oficial de Seguridad de BMCert es responsable de asegurar que las acciones correctivas se toman dentro de los 30 días. En ese momento, o antes, si así se acuerda por el Oficial de Seguridad de BMCert y Compliance Auditor, el equipo de auditoría de cumplimiento realizará la re-auditoría del servicio de EC en las áreas de deficiencias. Si, al volver a realizar la auditoría, no se han tomado las medidas correctoras, el Oficial de Seguridad de BMCert va a determinar qué acción debe ser tomada, y si (por ejemplo, la acción 3 o 4) se requiere una acción más severa.

2. Si no se toma acción 2, el Oficial de Seguridad de BMCert es responsable de garantizar que la ER no aprobará ninguna solicitud de certificado presentada después de la determinación de cesar la emisión de nuevos certificados. Por otra parte, deben expedirse los certificados después de que se hizo la determinación, pero antes de la finalización de una auditoría de cumplimiento con éxito, la ER tiene la responsabilidad de revocar los certificados afectados, con la razón de la revocación establecida en “sustituido”.

3. Si se toma la acción 3, el Oficial de Seguridad de BMCert es responsable de asegurar que CRLs y ARLs se publiquen según lo programado y la revocación de certificado se sigue realizando según sea necesario, sin embargo, no se realizan otras acciones de administración de usuarios (es decir, inscribir nuevos usuarios, emitir certificados, actualizar Certificados, etc.) por parte de la ER y los métodos alternativos y temporales de autenticación del usuario se ponen a disposición de los usuarios afectados por la decisión de suspender las operaciones.

4. Si se toma la acción 4 el Oficial de Seguridad de BMCert efectuará la revocación del certificado de la EC BMCert. Antes de la revocación del certificado del PKI original, un nuevo PKI se establecerá y deberá adherirse a los requisitos definidos en el CP BMCert

y esta CPS. Una vez que la nueva EC ha sido certificada como operacional, el Oficial de Seguridad de BMCert y sus asociaciones regionales y autoridades locales y regionales delegadas serán re-autenticadas considerando a cada suscriptor a la PKI original y se moverán (es decir, exportará la información del suscriptor incluyendo su clave histórica de la EC, después de que la base de datos de la EC ha sido validada para ser exactos y muestra integridad, y luego será importada en otra EC) al nuevo PKI. Sólo aquellos suscriptores que lograron volver a autenticarse en el cumplimiento de la BMCert CP serán reinscritos en el nuevo PKI. Este procedimiento preservará historias claves del Suscriptor y servirá para validar la integridad y exactitud de los suscriptores inscritos en el antiguo PKI. El Oficial de Seguridad de BMCert es responsable de asegurar que todos los suscriptores de la PKI originales son notificados de la terminación pendiente y reemisión de certificados PKI. No hay nuevos suscriptores que serán emitidos por la PKI originales; todas las nuevas solicitudes de certificados se presentarán al nuevo PKI para la emisión. Después de un período de 90 días, todos los certificados emitidos por los PKI originales serán revocados, si los suscriptores se han migrado a la nueva PKI y el proceso de terminación EC será seguido de la PKI originales.

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

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

El auditor entregará a la AAC un informe técnico sustentando las acciones a realizar y la AAC determinará cuál de estas acciones basada en la severidad de las irregularidades a ser tomada.

8.6. Comunicación de resultados

El Auditor de Cumplimiento comunicará los resultados de las auditorías de cumplimiento de servicio al Oficial de Seguridad de BMCert a través de un informe de auditoría de cumplimiento. El informe contendrá una tabla resumen de los temas tratados, áreas de incumplimiento de las disposiciones en las que se encontró que la PKI no cumple las disposiciones, una breve descripción del problema (s) para cada área de incumplimiento, y las posibles soluciones para cada área. El informe también contendrá los resultados detallados de la auditoría de cumplimiento de todos los temas tratados, incluyendo los temas en los que hayan superado la EC y los servicios de la EC y los temas en los que la EC y sus servicios fallaron.

La notificación de error de auditoría de cumplimiento, los temas de la falta, la razón (s) para el fracaso, y los posibles remedios se comunicarán de inmediato, tras la conclusión de la auditoría de cumplimiento, en forma escrita a el Oficial de Seguridad de BMCert.

9. OTROS ASUNTOS LEGALES Y COMERCIALES

9.1. Tarifas

9.1.1. Tarifas de emisión o renovación de certificados

La Entidad de Certificación BMCert de BMTECH PERU S.A.C. se somete al marco tarifario establecido por Indecopi para la acreditación y los procesos de auditoría respectivos, a fin de poder participar dentro del marco de la Infraestructura Oficial de Firma Electrónica.

9.1.2. Tarifas de acceso al certificado

La EC BMCert no aplica tasa para el acceso a la información del certificado.

9.1.3. Tarifas de acceso a la información de estado o revocación

La EC BMCert no aplica tasa para el acceso a la información del certificado.

9.1.4. Tarifas por otros servicios

El acceso a información de las Políticas y a la Declaración de Prácticas de Certificaciones libre y gratuito.

Las tarifas aplicables a otros servicios adicionales se acordarán directamente entre la EC BMCert y los clientes de otros servicios ofrecidos.

9.1.5. Política de reembolso

La Política de Reembolso de la EC BMCert se encuentra en su Repositorio www.bmcert.pe/documentos

La misma comprende:

La Política de Reembolsos de la EC BMCert refiere a los Certificados Digitales que emite bajo cualquiera de sus Políticas de Certificación.

La EC BMCert podrá otorgar un reembolso de la totalidad del importe abonado por el solicitante para los certificados con fallos u errores, o la emisión de un nuevo certificado sin costo alguno cuando:

- El solicitante presenta un reclamo sobre dicho certificado dentro de los 15 días posteriores a su fecha de emisión, y
- dicho reclamo obedece a una falla en el certificado u error en la emisión del mismo por parte de la EC BMCert.

Pasados los 15 días posteriores a la fecha de emisión del certificado, se entenderá total aceptación del certificado emitido y del servicio brindado por la EC BMCert, y no se realizarán reembolsos ni devoluciones de ningún tipo.

9.2. Responsabilidad financiera

9.2.1. Cobertura de seguro

No aplica

9.2.2. Otros activos

La EC BMCert posee suficientes recursos financieros para mantener sus operaciones y ejecutar sus deberes, y es capaz de administrar el riesgo de responsabilidad para los suscriptores y partes que confían.

9.2.3. Cobertura de seguro o garantía para entidades finales

No aplica.

9.3. Confidencialidad de la información comercial

La AAC garantiza que la información que mantiene relativa a las operaciones comerciales o de propiedad intelectual de los PSCs acreditados es mantenida de manera confidencial.

9.3.1. Alcance de la información confidencial

En todos los casos, la EC BMCert, empleados, profesionales y socios comerciales contratados mantienen en exclusiva reserva la información siguiente:

- Material comercialmente reservado de los Prestadores de Servicios de Certificación Digital, de los suscriptores, titulares y de los 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 existentes entre los suscriptores, titulares y los terceros que confían;
- Información que pueda permitir a personas no autorizadas la construcción de un perfil de las actividades de los suscriptores, titulares o terceros que confían;
- Toda información que pudiera perjudicarla normal realización de sus operaciones.

Conforme a lo establecido Indecopi, se permite la publicación de información respecto a la revocación de un certificado digital, sin revelar la causal que motivó dicha revocación. La publicación se encontrará restringida a suscriptores, titulares o terceros que confían.

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

Toda la información contenida en los certificados (siempre que el suscriptor lo autorice en el contrato del suscriptor) e información de estado de certificados, así como de

información en relación a la revocación de un certificado sin revelar la razón de dicha revocación será clasificada como “no confidencial”.

9.3.3. Responsabilidad de proteger la información confidencial

Todo el personal de la EC BMCert y el tercer que confía están obligados a guardar secreto sobre la información clasificada como “confidencial”.

9.4. Privacidad de la información personal

La EC BMCert cumple con lo estipulado sobre protección de datos de la norma “Marco sobre Privacidad de APEC” y en la legislación vigente, conforme se encuentra plasmado en su Política y Plan de Privacidad.

9.4.1. Plan de privacidad

La EC BMCert implementa una Política de Privacidad de información de acuerdo con la normativa vigente. Dicha Política de Privacidad se encuentra publicada en su Repositorio www.bmtech.pe/documentos.

9.4.2. Información tratada como privada

Dentro de la información que la EC BMCert trata como privada, tenemos la siguiente:

- Información personal provista por los suscriptores, titulares y terceros que confían que no sea la autorizada para estar contenida en certificados digitales y repositorios;
- Información que pueda permitir a partes no autorizadas establecer la existencia o naturaleza de las relaciones existentes entre suscriptores, titulares y terceros que confían;
- Información que pueda permitir a personas no autorizadas la construcción de un perfil de las actividades de los suscriptores, titulares o terceros que confían;
- La publicación respecto de la revocación de un certificado digital se realizará sin revelar su causal.

La publicación de esta información estará restringida a suscriptores, titulares o terceros que confían, según corresponda.

9.4.3. Información no considerada privada

La EC BMCert podrá divulgar la información personal siempre que se trate de información considerada como pública o caso mediante consentimiento expreso de dicha persona brindado a través de medios no repudiables.

La AAC permite la publicación de certificados e información de estado de certificado y la publicación de información en relación a si un certificado ha sido suspendido o revocado, sin revelar la causal que motivó dicha suspensión o revocación.

9.4.4. Responsabilidad de proteger la información privada

La EC BMCert cumple con todos los requerimientos de confidencialidad y las leyes sobre protección de datos y confidencialidad de la información que fuere aplicable, así como la Norma “Marco sobre Privacidad de APEC”

9.4.5. Aviso y consentimiento para usar información privada

En los contratos con suscriptores se establecerán claramente el tipo de datos personales que serán recolectados, la forma en que éstos serán utilizados y protegidos, y los mecanismos para su revisión y corrección, las circunstancias bajo las cuales éstos serán divulgados, la manera de desagravios y las sanciones para las fallas en el cumplimiento del acuerdo con la parte o partes que utilizan o recolectan dichos datos. Asimismo se incorporarán en dichos contratos, el necesario consentimiento para la divulgación de datos específicos.

9.4.6. Divulgación de conformidad con un proceso judicial o administrativo

En todos los casos, la EC BMCert permitirá la revelación de la 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.

Cuando la solicitud de divulgación de información proviene de otra jurisdicción, serán de aplicación las leyes de asistencia mutua.

9.4.7. Otras circunstancias de divulgación de información

La EC BMCert permite a los suscriptores, titulares y terceros que confían solicitar la divulgación de la información que se ha provisto a terceros.

En todo caso, la divulgación de la información de datos personales se realizará de acuerdo a la Ley N° 29733 – Ley de Protección de Datos Personales

9.5. Derechos de propiedad intelectual

BMTECH PERU SAC es la propietaria del presente documento y de las aplicaciones de su sistema de certificación de digital. Quedan excluidos los derechos de propiedad intelectual e industrial derivados de aplicaciones que integran el sistema de certificación digital y que sean propiedad de un tercero.

En todos los casos, la EC BMCert permite el acceso necesario a Indecopi de información de registro, nombres, claves, información de certificados digitales y repositorio, incluyendo copias del archivo que se encuentra disponible, a efectos de continuar las operaciones del mismo en el caso de eliminación o falla de los PSCs.

9.6. Representaciones y garantías

9.6.1. Declaraciones y garantías de EC

La EC BMCert garantiza que:

- No se presentan distorsiones en la información contenida en los certificados o en la emisión de los mismos.
- No existen errores en la información que fue introducida por la entidad que aprueba la emisión del certificado.
- Los certificados reúnen los requerimientos expuestos en este documento.
- Los servicios de revocación y el uso de los Repositorios cumplen lo estipulado en este documento.

9.6.2. Representaciones y garantías de ER

No aplica.

9.6.3. Declaraciones y garantías de los suscriptores

Las obligaciones de los suscriptores son:

- Entregar información veraz que permita su identificación personal o la verificación de algún tipo de atributo en particular, asumiendo responsabilidad por la veracidad y exactitud de dicha información.
- Generar la clave privada del certificado digital que le fuera emitido conforme al procedimiento que para tales efectos establezca la EC correspondiente.
- Respetar los términos del acuerdo o convenio celebrado con la ER que se encuentra acreditada ante la AAC para efectos de la prestación de servicios de certificación digital, según corresponda.
- Mantener el control y reserva de la clave privada, bajo responsabilidad.
- Observar las condiciones establecidas por esta EC para la utilización del certificado digital y generación de las firmas digitales.
- En caso que la clave privada quede comprometida en su seguridad, debe notificar este hecho de inmediato a la EC.
- Utilizar el certificado digital para los fines concretos para los cuales fuera emitido.
- Actualizar permanentemente la información proveída tanto a la EC como a la ER, asumiendo responsabilidad por la veracidad y exactitud de dicha información.
- Solicitar de inmediato la revocación de su certificado digital en caso la reserva sobre la clave privada se haya visto comprometida, bajo responsabilidad.
- Observar permanentemente las condiciones establecidas por la EC para la utilización del certificado digital, conforme a los términos establecidos en su CP/CPS y en el correspondiente contrato o convenio que hubiere celebrado para tales efectos.
- No manipular técnicamente la implementación de la infraestructura de clave pública a la cual corresponda el certificado digital del cual es titular ni realizar ingeniería inversa

o comprometer en cualquier modo intencional la seguridad de la misma o de la plataforma que pudiera tener la ER para efectos de la prestación de sus servicios de certificación digital

El suscriptor será responsable por los daños y perjuicios causados a EC BMCert. o a terceros por el incumplimiento de alguna de sus obligaciones a que se aluden en el presente documento

BMTECH PERU S.A.C. se reserva el derecho de iniciar las acciones judiciales civiles y penales que pudieran corresponderle por cualquier daño o perjuicio causado.

El suscriptor firmará un acuerdo de cumplimiento de sus obligaciones con la ER. En dicho acuerdo estarán contenidas las consecuencias de eventuales incumplimientos. El acuerdo contemplará las obligaciones establecidas por la legislación vigente.

Cuando un suscriptor celebra acuerdos en representación de varios titulares, sus responsabilidades en relación a las acciones de dichos titulares, también se encontrarán claramente establecidas en cada acuerdo. La ER pondrá a disposición de los titulares y suscriptores que se encuentren fuera de esta jurisdicción las obligaciones que deben cumplir.

9.6.4. Representaciones y garantías de la parte que confía

Las partes que confían deben:

- Tener pleno conocimiento de las garantías y responsabilidades aplicables en la aceptación y uso de los certificados en los que confía, y aceptar sujetarse a las mismas.
- Limitar la fiabilidad de los certificados a los usos permitidos de los mismos, de conformidad con la Política de Certificación pertinente.
- Verificar la validez de los certificados en el momento de realizar cualquier operación basada en los mismos, asumiendo su responsabilidad en la correcta comprobación de su estado.

9.6.5. Representaciones y garantías de otros participantes

Otros participantes no específicamente mencionados anteriormente, establecerán en su declaración de prácticas u otra documentación relevante, provisiones sobre garantías y responsabilidades, incluyendo limitaciones y exclusiones de las mismas. Dichas provisiones serán incluidas en todo contrato de suscriptor o tercero que confía

9.7. Renuncias de garantías

BMTECH PERU S.A.C. no asume ninguna exención de garantía o responsabilidad que no esté contemplado en este documento, se deba a caso fortuito o fuerza mayor, tales como desastres naturales o de otro tipo, cortes indebidos del suministro eléctrico o

funcionamiento defectuoso de los sistemas telemáticos que no sean factibles de resolver a través de las medidas de seguridad estándar que emplea la EC BMCert para la realización de sus funciones a excepción de aquellas garantías establecidas por la legislación vigente o por la normatividad de la AAC.

9.8. Limitaciones de responsabilidad

BMTECH PERU S.A.C. no asume ninguna responsabilidad que no esté contemplado en este documento, se deba a caso fortuito o fuerza mayor, tales como desastres naturales o de otro tipo, cortes indebidos del suministro eléctrico o funcionamiento defectuoso de los sistemas telemáticos que no sean factibles de resolver a través de las medidas de seguridad estándar que emplea la EC BMCert para la realización de sus funciones a excepción de aquellas garantías establecidas por la legislación vigente o por la normatividad de la AAC.

9.9. Indemnizaciones

BMTECH PERU S.A.C. se sujetará a lo establecido para tales efectos en los convenios que pudiera mantener como EC correspondiente y se encontrará debidamente referenciada en cada uno de los contratos con suscriptores y titulares u documentación correspondiente en lo que atañe a sus relaciones con los terceros que confían.

9.10. Duración y rescisión

9.10.1. Plazo

El periodo de validez máximo del presente documento es de tres (3) años, lo mismo que será modificado conforme lo determine la AAC o la propia EC. En todos los casos cualquier modificación que se efectúe será debidamente comunicada a los suscriptores, titulares y, de ser el caso, terceros que confían.

En caso que caducara la acreditación de la EC BMCert, se entiende que su documentación también ha caducado en lo que atañe a las operaciones realizadas dentro de la Infraestructura Oficial de Firma Electrónica.

Las provisiones antes señaladas serán incluidas en los contratos del suscriptor, titular y de ser el caso, en los contratos de los terceros que confían.

9.10.2. Terminación

La EC BMCert informará a la AAC sobre el cese de sus operaciones con treinta (30) días de anticipación, de acuerdo a los procedimientos establecidos por dicha entidad.

9.10.3. Efecto de la terminación y supervivencia

Cada uno de los puntos en el presente documento tiene la naturaleza de ser independiente. En tal sentido, la eventual declaratoria de nulidad o invalidez de alguno de ellos, no

generará la nulidad de todo el documento.

De igual manera las cláusulas incorporadas en los contratos de suscriptores o Términos PKI u otro tipo de documentación suscrita con terceros que confían serán independientes entre sí. En tal sentido la eventual declaratoria de nulidad de cualquiera de las cláusulas no generará la nulidad o invalidez de todo el contrato.

9.11. Avisos individuales y comunicaciones con los participantes

Para todas las comunicaciones entre la EC BMCert y sus asociados, suscriptores y terceros que confían, se tendrá como referencia el domicilio real o electrónico señalado en los correspondientes contratos, en donde se tendrán por válidamente realizadas todas las comunicaciones realizadas.

9.12. Enmiendas

9.12.1. Procedimiento de modificación

Cualquier cambio al presente documento, la EC BMCert consultará con la AAC antes de poder implementarlo. Esto no aplica en los casos en que dichos cambios sean consistentes con las operaciones documentadas de la propia IOFE (AAC).

9.12.2. Mecanismo y período de notificación

Cualquier cambio al presente documento, la EC BMCert consultará con la AAC una vez aprobada por la AAC, será notificada a los asociados de negocio, suscriptores, terceros que confían y otras partes de tales como otras infraestructuras que reconocen a la Ec de BMCert, así como acuerdos de certificación cruzada, siempre que dichos cambios puedan afectarles.

La ER notificará esto a los domicilios reales o electrónicos que para tales efectos hayan establecido los suscriptores y terceros que confían la forma de notificación de esta información.

Las modificaciones antes señaladas serán notificadas también a través de la página web.

9.12.3. Circunstancias bajo las cuales se debe cambiar el OID

Cualquier cambio en el OID de cualquiera de los certificados y políticas será aprobado previamente por la AAC.

9.13. Disposiciones de resolución de disputas

En la eventualidad de cualquier disputa que implique los servicios o prestaciones que incluye este documento, la parte afectada notificará primero la EC y a todas las partes interesadas con relación a la disputa. La EC asignará al personal adecuado para resolver dicho reclamo.

Agotada esta vía ante la EC, en caso de no encontrarse conforme, el reclamante podrá recurrir en vía administrativa a la AAC, con sujeción a lo establecido para tales efectos por la Ley No. 27444 – Ley del Procedimiento Administrativo General.

9.14. Ley aplicable

La ley aplicable para todos los efectos del presente documento son las leyes peruanas, principalmente la Ley N° 27269, Ley de Firmas y Certificados Digitales, y su Reglamento, así como las disposiciones contenidas en la Guía de Acreditación de Entidad de Certificación (EC) y sus anexos, el Reglamento General de acreditación de Prestadores de Servicios de Certificación Digital y el Reglamento Específico de Acreditación de entidad de Certificación (EC) aprobados por Resolución de la Comisión de Reglamentos Técnicos y Comerciales del Indecopi Nº 030-2008/CRT-INDECOPI. Así como lo establecido mediante Decreto Supremo Nº 070-2011-PCM. Los requerimientos legalmente significativos se encuentran debidamente establecidos y referenciados en los contratos de suscriptores, titulares y de ser el caso, terceros que confían.

9.15. Cumplimiento de la ley aplicable

Las provisiones estipuladas en el presente documento han sido establecidas en conformidad con la Ley N° 27269, Ley de Firmas y Certificados Digitales, y su Reglamento, aprobado por el Decreto Supremo 052-2008-PCM y la Guía de Acreditación de Entidad de Certificación (EC)) y sus anexos, el Reglamento General de acreditación de Prestadores de Servicios de Certificación Digital y el Reglamento Específico de Acreditación de entidad de Certificación (EC) aprobados por Resolución de la Comisión de Reglamentos Técnicos y Comerciales del Indecopi Nº 030-2008/CRT-INDECOPI

9.16. Disposiciones varias

Las cláusulas se encuentran debidamente establecidas y referenciadas en los contratos de suscriptores, titulares y, de ser el caso, terceros que confía.

9.16.1. Acuerdo completo

Todas las entidades finales, suscriptor y terceros que confían, vinculadas a través de convenios, asumen la aceptación en su totalidad el contenido de la última versión de este documento que les sean aplicables. Así como la el presente documento u otra documentación que rija las relaciones con los terceros que confían, serán los únicos instrumentos jurídicos encargados de regir las funciones, obligaciones y responsabilidades entre estos sujetos.

9.16.2. Asignación

Los derechos y los deberes de la EC BMCert no podrán ser objeto de cesión a terceros de ningún tipo, ni ninguna tercera entidad podrá subrogarse en la posición jurídica de esta

entidad.

Cuando un contrato de suscriptor cubre a múltiples titulares, toda limitación en la subrogación de derechos o delegación de obligaciones a dichos titulares se encontrará debidamente establecida en dicho acuerdo.

9.16.3. Divisibilidad

La EC BMCert conjuntamente con las ER con las que trabaje, establecerán en sus contratos de suscriptor y terceros que confían cláusulas de divisibilidad, por las cuales la invalidez de una cláusula no afectará al resto del contrato.

9.16.4. Ejecución (honorarios de abogados y renuncia de derechos)

Las cláusulas de ejecución establecidas por la EC BMCert, serán referenciadas en los contratos de suscriptores, titulares y, de ser el caso, terceros que confía.

9.16.5. Fuerza mayor

La EC BMCert conjuntamente con las ER con las que trabaje, se asegurarán que las cláusulas de "fuerza mayor" sean establecidas explícitamente en los contratos de suscriptor y terceros que confían.

9.17. Otras disposiciones

No aplica.