SERVICIOS ADMINISTRADOS POR ENTRUST

Declaración de Prácticas y Políticas de Certificación para Infraestructuras de Clave Pública X.509 (EC BMCert)

VERSIÓN 1.1

Fecha: 04 de enero, 2020

SERVICIOS ADMINISTRADOS POR ENTRUST

Certificaciones	Emitido Por	Fecha Emisión
ISO 27001 – Certificado N° SEC1568	A-LIGN	04 de Marzo de 2016
WEBTRUST	Deloitte LLP	03 de Junio de 2016

Este CPS es un documento que detalla los procedimientos usados para la emisión y cancelación de certificados digitales. Se escribe para ser utilizado conjuntamente con el siguiente documento, que por referencia forman parte de este CPS:

- *Arquitectura V1.0 de la EC BMCert MSO PKI*. Este documento describe los requisitos funcionales de la EC BMCert PKI y la arquitectura técnica.

Este CPS es gobernado por la CP de EC BMCert (*Política de Certificación para la infraestructura de clave pública X.509 (EC BMCert),* que es parte del documento *X.509 Certificate Policy for the Entrust Managed Services Commercial Public Key Infrastructure (EMS CCP)*, versión 1.6, del 1 de noviembre de 2010.

Lima, 08 de Agosto 2017

EXPEDIENTE DE CAMBIOS

Versión	Fecha	Autores	Descripción
0.1 Borrador	18 de febrero, 2016	M. Bouchard Entrust PS.	Primer esbozo para la revisión de la EC BMCert.
0.2	06 de junio 2017	M. Bouchard Entrust PS.	Actualización Documento – Proceso de Acreditación
1.0 Final	08 de agosto 2017	Luis Bays BMTECH	Versión final.
1.1	04 de enero 2020	Luis Bays BMTECH Axell Alvarado BMTECH	Agregados nuevos perfiles de certificados de persona natural con negocio y persona natural profesional

SERVICIOS ADMINISTRADOS POR ENTRUST

Acerca de Entrust:

Una compañía de prestígio global con oficinas en 35 paises y presencia en más de 150 países, con más de 20 años ofreciendo su solución de PKI, con experiencia en Gobierno, bancos, saludo y otras empresas..

Actualmente son más de 100 patentes relacionadas con autenticación y PKI y reconocidos como pioneros y líderes en PKI a nivel global, Entrust fue el primer fabricante en recibir la acreditación FIPS 140-2 del gobierno de los Estados Unidos en 1995 y también fue el primer proveedor de PKI en obtener la certificación de Common Criteria EAL 4 de ISO en 1999 y nuevamente en 2012, en los certificados SSL, también fueron el primer proveedor en obtener el sello “WebTrust”.

Entrust tambien fue la consultora que reviso y indico sugerencias compatibles con la normativa peruana y agregadas al proyecto del documento principal –el proyecto de “Guía de Acreditación de Entidades de Certificación Digital– y que tuvo participación en el diseño de la Infraestructura de Firma Digital de la administración del Estado del Canadá.

Contenido

1.0 INTRODUCCIÓN

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 Entrust y 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.

La CPS de la EC BMCert es un documento que consolida las prácticas observadas por la EC BMCert, y las prácticas Entrust adecuadas como parte de las operaciones PKI. Este documento se debe leer y aplicarse conjuntamente con la "(*Declaración de Prácticas y Políticas de Certificación para Infraestructuras de Clave Pública X.509 Servicios Comerciales Públicos Administrados por Entrust (en inglés – EMS CPPKI CPS)"* para el Managed Service Offering (MSO) que es el operador de la EC BMCert. Sin embargo, este documento (también identificado por *EMS CPPKI CPS)* contiene información que no es relevante a las prácticas del cliente (así como contiene información que es propietaria de Entrust), este documento fue creado para permitir incorporar a la EC BMCert esas políticas y procedimientos relevantes.

Este CPS es aplicable y público a todas las entidades relacionadas con la EC BMCert, incluyendo suscriptores, partes que confían (terceros usuarios), Entidades de Registro (ERs). Este CPS provee un resumen claro de las prácticas y de las responsabilidades de la EC BMCert con respecto a dichas ERs, así como de las responsabilidades de cada entidad final que tenga relación con la EC BMCert.

Este CPS es un documento de los procedimientos que discute las políticas de implementación. Se escribe para ser utilizado conjuntamente con los siguientes documentos, que por referencia forman parte de este CPS:

- *Arquitectura V1.0 de la EC BMCert MSO PKI*. Este documento describe los requisitos funcionales de la EC BMCert PKI y la arquitectura técnica.
- *Registro de la Declaración de las Prácticas de la EC BMCert V1.0*.

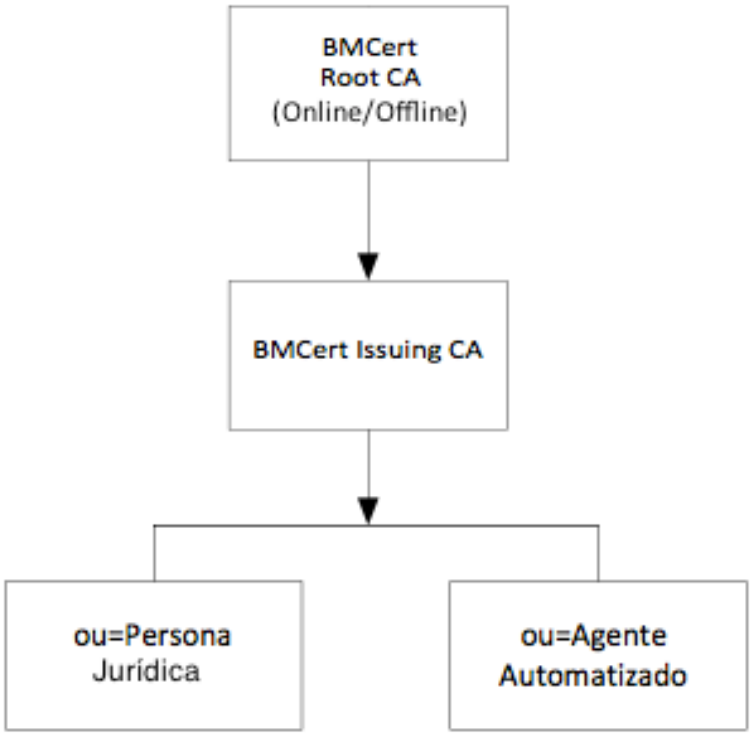
Este CPS es gobernado por la *política del certificado X.509 para la infraestructura de clave pública de la EC BMCert (BMCert CP/CPS),* que es un documento de la *política del certificado X.509 para los Servicios Comerciales Administrados por Entrust de infraestructura de clave pública (EMS CCP)*, versión 1.6, del 1 de noviembre de 2010.

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 la Infraestructura de Clave Pública (PKI) que es operado por el MSO. La PKI consiste de una EC Raíz auto fimada, una EC on-line subordinada (ejemplo, 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.

1.1.1 Clases de Certificados

La infraestructura de clave pública de la EC BMCert emite y gestiona diferentes clases de certificados digitales de acuerdo al tipo de suscriptor o entidad final. Inicialmente clasificados de la siguiente manera:



Se podrá generar una Raíz BMCert Root CA off-line para ECs intermedias off-line en casos de contingencia previstos tanto para la raíz BMCert Root CA on-line como para limitaciones de acceso a internet por parte de la Entidad final (usuario final) a fin de proveer los servicios de certificación digital en esas condiciones.

1.2 Nombre e identificación del documento

Nombre del documento	Declaración de Prácticas y Políticas de Certificación para Infraestructuras de Clave Pública X.509 (EC BMCert)
OID	2.16.840.1.114027.200.3.10.39
Versión del documento	1.1
Estado del documento	Versión Final
Fecha de emisión	04 de Enero 2020
Publicación de la CPS	https://www.bmtech.pe/repositorio/

1.3 Participantes

La comunidad de usuarios se compone, en primera instancia, por aquellas personas naturales y jurídicas que obtienen y utilizan un certificado digital emitido por una EC acreditada con la intervención de una ER acreditada, dichos usuarios deben cumplir los requerimientos especificados en las siguientes secciones de este documento y otros, como la correspondiente Declaración de Prácticas de Registro - DPR. Se consideran casos de contingencia en la EC off-line.

Las prácticas descritas en esta CPS son gobernadas y desarrolladas para respaldar el CP de la EC BMCert.

1.3.1 Entidades de Certificación

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

La EC BMCert es la entidad encargada de la emisión y revocación de certificados digitales de

Personas Naturales, 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 cancelación de certificados digitales.

Las prácticas definidas en esta CPS están relacionadas y gobiernan la operación y mantenimiento de las Entidades Certificadoras Raíz y Subordinadas on-line específicamente y son referentes para la provisión de los servicios off-line de ser el caso.

La EC BMCert Raíz (BMCert Root CA – on-line/off-line) emite Certificados a la EC BMCert subordinada (BMCert Issuing CA) o la que corresponda en el modo off-line.

1.3.2 Entidades de Registro

La EC BMCert tiene convenio y vínculo con la ER IOFE S.A.C., de igual manera se tiene con la ER Gramd Peruana S.A.C. y asimismo, puede proveer sus servicios a través de cualquier ER acreditada.

1.3.3 Titulares de certificados

Son titulares de los certificados digitales las personas jurídicas principalmente.

Personas naturales: Aquellas que puedan sustentar su existencia y se encuentran registradas en las Base de Datos de la Reniec. Las personas naturales asumen la responsabilidad de titulares de los certificados que adquieren. En este caso existen dos tipos de suscriptores: la persona natural como tal, y la persona natural con profesión. En el certificado de la persona natural quedarán registrados su identidad, los cuales le permitirán utilizar el certificado para realizar transacciones en su propio nombre. Por otro lado, los certificados de las personas naturales con profesión quedarán registradas de acuerdo a la profesión que acrediten con la respectiva verificación del Colegio Profesional.

Personas jurídicas: Aquellas que puedan sustentar su existencia y se encuentren registradas en los Registros Públicos. Las personas jurídicas asumen la responsabilidad de titulares de los certificados que adquieren. En este caso existen dos tipos de suscriptores: el representante legal y los funcionarios o empleados, dependientes o designados por la PPJJ para asumir algún rol o propósito específio en el marco de un proceso temporal o definitivo, que por el cargo que ocupan deben adquirir un certificado digital. En el certificado del representante legal quedarán registrados sus atributos, los cuales le permitirán utilizar el certificado para realizar transacciones en nombre de la persona jurídica. Por otro lado, los certificados de los funcionarios, empleados o dependientes tienen atributos limitados al desenvolvimiento de sus funciones dentro de la persona jurídica.

Tratándose de certificados digitales solicitados por personas jurídicas para su utilización a través de agentes automatizados, la titularidad de certificados y de las firmas digitales generadas a partir de dicho certificado corresponderá a la persona jurídica. La atribución de responsabilidad, para tales efectos, corresponde al representante legal, que en nombre de la persona jurídica solicita el certificado digital.

1.3.4 Tercero que confía (terceros usuarios)

Los terceros que confían o terceros usuarios son aquellas personas naturales o jurídicas (diferentes al titular o suscriptor del certificado digital), equipos, servicios 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

Todas las funciones, operaciones y actividades de la Entidad Certificadora BMCert, que tiene su servicio bajo contrato de servicio MSO Entrust.

Todas las funciones, operaciones y actividades de Entidad de Registro y Verificación corresponden a IOFE S.A.C. a la cual está vinculada; o de cualquier otra ER que se encuentre acreditada ante la AAC.

1.3.5.1 SVAs

No Aplica.

1.4 Uso del certificado

El siguiente cuadro resume los tipos de certificados y sus usos:

Clase	Tipo de persona que lo usa	Vigencia	Longitud de la clave	Modo de generacion	Uso
Clase I	Jurídica	1, 2 y 3 años	2048	Automático	▪ Autenticación y firma
Clase II	Jurídica (Agente Automatizado)	1, 2 y 3 años	2048	Automático	▪ Autenticación y firma
Clase III	Natural	1, 2 y 3 años	2048	Automático	▪ Autenticación y firma
Clase IV	Natural con Negocio	1, 2 y 3 años	2048	Automático	▪ Autenticación y firma
Clase V	Natural Profesional	1, 2 y 3 años	2048	Automático	▪ Autenticación y firma

Detalle de los tipos de certificados emitidos por la EC BMCert y su clasificación:

a) Por el titular:

Certificados de Persona Jurídica

Se caracteriza porque el poseedor actúa a nombre y representación de la persona jurídica. La persona jurídica considera los siguientes actores: titular que es el representante legal y funcionarios autorizados que son los suscriptores del certificado digital.

Dentro de este tipo existen 2 clases:

- Clase I para personas naturales que actúan en representación de la persona jurídica.
- Clase II, emitidos para equipos servidores (persona jurídica).

Certificados de Persona Natural

Se caracteriza porque el poseedor actúa a nombre y representación de sí mismo en calidad de persona natural.

Dentro de este tipo existen 4 clases:

- Clase III para personas naturales que actúan en representación de sí mismas.
- Clase IV para personas naturales que cuentan con negocio y RUC propio.

- Clase V, emitidos para equipos servidores (persona natural).
- Clase VI para personas naturales profesionales que cuentan con colegiatura.

b) Por el uso:

Por el uso que se le da al certificado digital, este se puede clasificar en:

i. Certificados de autenticación y firma digital: son utilizados para control de acceso y permisos donde se requiera autenticar a un suscriptor, y adicionalmente pueden ser utilizados en transacciones electrónicas que requieran la firma digital del suscriptor del certificado.

Se podrá generar una Raíz BMCert Root CA off-line para ECs intermedias off-line en casos de contingencia previstos tanto para la raíz BMCert Root CA on-line como para limitaciones de acceso a internet por parte de la Entidad final (usuario final).

1.4.1 Uso apropiado del certificado

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

- **Certificado de Autenticación y Firma**: El uso conjunto de ambos certificados proporciona las siguientes garantías:

i. Autenticidad de origen

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

ii. No repudio de origen

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

iii. Integridad

Con el empleo del Certificado de Firma, se puede garantizar que un documento electrónico no ha sido alterado desde la transmisión por el emisor hasta su recepción por el destinatário

1.4.2 Prohibiciones del uso del certificado

El certificado no se puede usar para fines o aplicaciones no contemplados en 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 los documentos de CPS o CP

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: Calle Grimaldo del Solar, 162, Of. 1002, Miraflores, Lima, Lima, Peru
Teléfono: 01 2461991

1.5.2 Persona de contacto

Nombre: Luis Bays
Dirección de correo: luis@bmtech.pe
Dirección: Calle Grimaldo del Solar, 162, Of. 1002, Miraflores, Lima, Lima, Peru
Teléfono: 01 2461991

1.5.3 Persona que determina la conformidad 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 Procedimiento de aprobación de CPS

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

1.6 Definiciones y acrónimos

Definiciones:

Definiciones según el D.S. 052-2008-PCM "Reglamento de la Ley de Firmas y Certificados Digitales".

Acreditación	Es el acto a través del cual la AAC, previo cumplimiento de las

	exigencias establecidas en la Ley, el Reglamento y las disposiciones dictadas por ella, faculta a las entidades solicitantes a prestar los servicios solicitados en el marco de la Infraestructura Oficial de Firma Electrónica
Agente Automatizado	Son los procesos y equipos programados para atender requerimientos predefinidos y dar una respuesta automática sin intervención humana, en dicha fase.
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.
Archivo Electrónico	Es el conjunto de registros que guardan relación. También es la organización de dichos registros.
Autenticación	Es el proceso técnico que permite determinar la identidad de la persona que firma digitalmente, en función del documento electrónico firmado por éste y al cual se le vincula; este proceso no otorga certificación notarial ni fe pública.
Autoridad Administrativa Competente	Es el organismo público responsable de acreditar a las Entidades de Certificación, a las Entidades de Registro o Verificación y a los Prestadores de Servicios de Valor Añadido, públicos y privados, de reconocer los estándares tecnológicos aplicables en la Infraestructura Oficial de Firma Electrónica, de supervisar dicha Infraestructura, y las otras funciones señaladas en el presente 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.
Certificación Cruzada	Es el acto por el cual una Entidad de Certificación acreditada reconoce la validez de un certificado emitido por otra, sea nacional, extranjera o internacional, previa autorización de la AAC; y asume tal certificado como si fuera de propia emisión, bajo su responsabilidad.
Certificado Digital	Es el documento credencial electrónico generado y firmado digitalmente por una Entidad de Certificación que vincula un par de claves con una persona natural o jurídica confirmando su identidad.
Clave privada	Es la clave en un sistema de criptografía asimétrica que es usada por el destinatario de un documento electrónico para firmar un documento. La clave privada sólo debe permanecer en propiedad del suscriptor.
Clave pública	Es la otra clave en un sistema de criptografía asimétrica que es usada por el destinatario de un documento electrónico para verificar la firma digital puesta en dicho documento. La clave pública puede ser conocida por cualquier persona.
HASH (Código de verificación o resumen criptográfico)	Es la secuencia de bits de longitud fija obtenida como resultado de procesar un documento electrónico con un algoritmo, de tal manera que: (1) El documento electrónico produzca siempre el mismo código de verificación (resumen) cada vez que se le aplique dicho algoritmo. (2) Sea improbable a través de medios técnicos, que el documento electrónico pueda ser derivado o reconstruido a partir del código de verificación (resumen) producido por el algoritmo. (3) Sea improbable por medios técnicos, que se pueda encontrar dos documentos electrónicos que produzcan el mismo código de

	verificación (resumen) al usar el mismo algoritmo.
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)	Es el documento oficialmente presentado por una Entidad de Certificación a la AAC, mediante el cual define sus Prácticas de Certificación
Declaración de Prácticas de Registro o Verificación (DPR)	Documento oficialmente presentado por una Entidad de Registro o Verificación a la AAC, mediante el cual define sus Prácticas de Registro o Verificación. Nota: en el presente documento se usará el acrónimo DPR para representar a los siguientes documentos: i. "*Declaración de Prácticas de Registro o Verificación"* para certificados digitales autorizados por alguna otra Entidad de Registro o Verificación acreditada por la AAC.
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.
Documento electrónico	Es la unidad básica estructurada de información registrada, publicada o no, susceptible de ser generada, clasificada, gestionada, transmitida, procesada o conservada por una persona o una organización de acuerdo a sus requisitos funcionales, utilizando sistemas informáticos.
Documento oficial de identidad	Es el documento oficial que sirve para acreditar la identidad de una persona natural, que puede ser: a) Documento Nacional de Identidad (DNI); b)Carné de extranjería actualizado, para las personas naturales extranjeras domiciliadas en el país; o, c) Pasaporte, si se trata de personas naturales extranjeras no residentes.
Entidad de Certificación	Es la persona jurídica pública o privada que presta indistintamente servicios de producción, emisión, gestión, cancelación u otros servicios inherentes a la certificación digital. Asimismo, puede asumir las funciones de registro o verificación.
Entidad de Registro o Verificación	Es la persona jurídica, con excepción de los notarios públicos, encargada del levantamiento de datos, la comprobación de éstos respecto a un solicitante de un certificado digital,la aceptación y autorización de las solicitudes para la emisión de un certificado digital, así como de la aceptación y autorización de las solicitudes de cancelación de certificados digitales. Las personas encargadas de ejercer la citada función serán supervisadas y reguladas por la normatividad vigente.
Entidad final	Es el suscriptor o propietario de un certificado digital.
Identificador de	Es una cadena de números, formalmente definida usando el

objeto (OID)	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, CPS, etc.).
Infraestructura Oficial de Firma Electrónica (IOFE)	Sistema confiable, acreditado, regulado y supervisado por la AAC, provisto de instrumentos legales y técnicos que permiten generar firmas digitales y proporcionar diversos niveles de seguridad respecto de: 1) La integridad de los documentos electrónicos; 2) La identidad de su autor, lo que es regulado conforme a Ley. El sistema incluye la generación de firmas digitales, en la que participan entidades de certificación y entidades de registro o verificación acreditadas ante la AAC incluyendo a la Entidad de Certificación Nacional para el Estado Peruano, las Entidades de Certificación para el Estado Peruano, las Entidades de Registro o Verificación para el Estado Peruano y los Prestadores de Servicios de Valor Añadido para el Estado Peruano.
Integridad	Es la característica que indica que un documento electrónico no ha sido alterado desde la transmisión por el iniciador hasta su recepción por el destinatario.
Interoperabilidad	Según el OASIS Forum Group la interoperabilidad puede definirse en tres áreas: • Interoperabilidad a nivel de componentes:consiste en la interacción entre sistemas que soportan o consumen directamente servicios relacionados con PKI. • Interoperabilidad a nivel de aplicación: consiste en la compatibilidad entre aplicaciones que se comunican entre sí. • Interoperabilidad entre dominios o infraestructuras PKI: consiste en la interacción de distintos sistemas de certificación PKI (dominios, infraestructuras), estableciendo relaciones de confianza que permiten el reconocimiento indistinto de los certificados digitales por parte de los terceros que confían.
Ley	Ley Nº 27269 - Ley de Firmas y Certificados Digitales, y sus modificatorias.
Lista de Certificados Revocados (CRL)	Es aquella en la que se deberá incorporar todos los certificados cancelados por la entidad de certificación de acuerdo con lo establecido en el presente Reglamento.
Niveles de seguridad	Son los diversos niveles de garantía que ofrecen las variedades de firmas digitales, cuyos beneficios y riesgos deben ser evaluados por la persona, empresa o institución que piensa optar por una modalidad de firma digital para enviar o recibir documentos electrónicos
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) - Distinguished Name (DN)	Es un sistema estándar diseñado para consignar en el campo sujeto de un certificado digital los datos de identificación 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 Entidad de Certificación. En inglés se denomina "Distinguished Name".
Par de claves	En un sistema de criptografía asimétrica comprende una clave privada y su correspondiente clave pública, ambas asociadas matemáticamente.
Políticas de Certificación	Documento oficialmente presentado por una Entidad de Certificación a la AAC, mediante el cual se 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 Entidad de Certificación Raíz, la Política de Certificación incluye las directrices para la gestión del Sistema de Certificación de las Entidades de Certificación vinculadas
Prácticas de Certificación	Son las prácticas utilizadas para aplicar las directrices de la política establecida en la Política de Certificación respectiva
Prácticas de Registro o Verificación	Son las prácticas que establecen las actividades y requerimientos de seguridad y privacidad correspondientes al Sistema de Registro o Verificación de una Entidad de Registro o Verificación
Reglamento	Reglamento Nº 052-2008–PCM de la Ley Nº 27269 - Ley de Firmas y Certificados Digitales, y sus modificatorias.
Servicio OCSP	Es el servicio que permite utilizar un protocolo estándar para realizar consultas en línea (on line) al servidor de la ER.
Suscriptor	Es la persona natural responsable de la generación y uso de la clave privada, a quien se le vincula de manera exclusiva con un documento electrónico firmado digitalmente utilizando su clave privada. En el caso que el titular del certificado digital sea una persona natural, sobre ella recaerá la responsabilidad de suscriptor. En el caso que una persona jurídica sea el titular de un certificado digital, la responsabilidad de suscriptor recaerá sobre el representante legal designado por esta entidad. Si el certificado está designado para ser usado por un agente automatizado, la titularidad del certificado y de las firmas digitales generadas a partir de dicho certificado corresponderán a la persona jurídica. La atribución de responsabilidad de suscriptor, para tales efectos, corresponde a la misma persona jurídica.
Tercero que confía o tercer usuario	Se refiere a las personas naturales, equipos, servicios o cualquier otro ente que actúa basado en la confianza sobre la validez de un certificado y/o verifica alguna firma digital en la que se utilizó dicho certificado.
Titular	Es la persona natural o jurídica a quien se le atribuye de manera exclusiva un certificado digital.
Usabilidad	En el contexto de la certificación digital, el término Usabilidad se aplica a todos los documentos, información y sistemas de ayuda necesarios que deben ponerse a disposición de los usuarios para asegurar la aceptación y comprensión de las tecnologías, aplicaciones informáticas, sistemas y servicios de certificación

	digital de manera efectiva, eficiente y satisfactoria
Usuario final	En líneas generales, es toda persona que solicita cualquier tipo de servicio por parte de un Prestador de Servicios de Certificación Digital acreditado
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 por sus siglas en inglés -ver Cica.ca) 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.

Otras definiciones

Entidad Raíz	Se encuentra en la cima de la pirámide de las Entidades permitidas para emitir certificados, su tarea específica es la de emitir certificados para Entidades Intermedias y generar la CRL para éstas. En el marco de la IOFE.
Entidad Intermedia	Se encuentra por debajo de una Entidad Raíz y es la encargada de emitir certificados para entidades finales (Personas Naturales o Jurídicas). En el marco de la IOFE.
Nombre distinguido	Es equivalente a Nombre diferenciado.
Nombre FQDN	Es el identificador que incluye el nombre de la computadora y el nombre de dominio asociado a ese equipo que puede identificar de forma única a un equipo servidor (o arreglo de estos) en el internet.
Nombre Común - (CN)	Es un atributo que forma parte del Nombre Distinguido (Distinguished Name - DN). Nombre de Dominio totalmente calificado - Fully Qualified Domain.
Identidad digital	Es el reconocimiento de la identidad de una persona en un medio digital (como por ejemplo Internet) a través de mecanismos tecnológicos seguros y confiables, sin necesidad de que la persona esté presente físicamente.
Hardware Security Module	Traducido al español es módulo de seguridad de hardware. Es un dispositivo criptográfico basado en hardware que genera, almacena y protege claves criptográficas. Aporta aceleración en las operaciones criptográficas.
Revocación de certificado digital	Anulación definitiva de un certificado digital a petición del suscriptor, un tercero o por propia iniciativa de la Entidad de certificación en caso de duda de la seguridad de las claves o por cualquier motivo permitido y debidamente sustentado descritos en la Declaración de Prácticas de Registro o Verificación.

Acrónimos:

AAC – Autoridad Administrativa Competente (CNB del INDECOPI)

AIA – Authority Information Access

ARL – Authority Revocation List

CC – Common Criteria

CDP – Certificate Distribution Point

CP – Políticas de Certificación

CPS – Declaración de Prácticas de Certificación de una EC

CRL o LCR – Certificate Revocation List (Lista de Certificados Revocados)

CWA – CEN Workshop Agreements

DCH – Device Certificate Holder (Titular del Certificado del dispositivo)

EAL – Evaluation Assurance Level

EC – Entidad de Certificación

EMS CPPKI CPS – *X.509 Certification Practices Statement for the Entrust Managed Services Commercial Public Public Key Infrastructure for the Entrust Managed Service Offering (MSO)*

ER – Entidad de Registro o Verificación (o sus Agencias, según sea el caso)

FIPS – Federal Information Processing Standards

GSA – General Services Administration (Administración de Servicios Generales)

HSPD – Homeland Security Presidential Directive (Directiva Presidencial de Seguridad Nacional)

IEC – International Electrotechnical Commission

IOFE – Infraestructura Oficial de Firma Electrónica

ISO – International Organization for Standardization

LDAP – Lightweight Directory Access Protocol

MSO – Managed Service Offering (Servicio de PKI Hosteado Entrust)

NIAP PP CIMC SL3 – National Information Assurance Partnership, Protection Profile, Certificate Issuing and Management Components, Security Level 3 (Asociación Nacional de Aseguramiento de la Información, Protección de Perfil, Emisión de certificados y gestión de componentes, Nivel de seguridad)

NTP – Network Time Protocol (Protocolo de tiempo de red)

OA – Operational Authority (Operador de la Entidad)

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

OID – Identificador de Objeto

PKI – Public Key Infrastructure (Infraestructura de Clave Pública)

PKIX-CMP – Public Key Infrastructure X Certificate Management Protocol

PPC – Primary Point of Contact (Primera Persona de Contacto)

PSC – Prestador de Servicios de Certificación Digital/Prestador de Servicios de Criptográficos

RFC – Request for Comment

DPR – Declaración de Prácticas de Registro o Verificación de una ER

SHA – Secure Hash Algorithm

SSAE – Statement on Standards for Attestation Engagements

SVA – Prestador de Servicios de Valor Añadido (por ejemplo TimeStamping)

SW – Software de Firma Digital

TA – Trusted Agents (Agente de confianza)

TSL – Lista de Estado de Servicio de Confianza

UPS – Uninterruptible Power Supply

XAP – XML Administration Protocol

2.0 PUBLICACION Y RESPONSABILIDADES DEL REPOSITORIO

2.1 Repositorios

El repositorio para la PKI BMCERT (EC BMCert) abarca los servicios siguientes:

1. Un directorio Lightweight Directory Access Protocol (LDAP) y se accede mediante el protocolo LDAP versión 3, según lo especificado en RFC 1777 del Internet.
2. Un Web site, gestionado por MSO, accesible a través de Internet mediante el protocolo de transferencia de hipertexto (http/https). Este repositorio hospeda los certificados de la EC y las CRLs.

2.2 Publicación de información sobre certificación

La EC BMCERT es responsable de la publicación de toda información referente a los certificados digitales emitidos por esta. Todas las ECs que emiten certificados bajo esta política están obligadas a publicar todos los certificados de la EC y todas las CRLs publicados por la EC en un directorio que es accesible desde la red de la EC BMCert e internet a través de los protocolos de LDAP y HTTP.

La EC BMCert puede distribuir esta documentación de acuerdo con sus directrices internas a todas las partes interesadas.

La EC BMCERT publica la siguiente información en los servidores HTTP hosteados por Entrust MSO:
Objetos de la raíz –BMCert Root CA:

- AIA: `http://bmcertcrl.managed.entrust.com/AIA/CertsIssuedtoBMCertRootCA.p7c`
- CDP: `http://bmcertcrl.managed.entrust.com/CRLs/BMCertRootCA.crl`

Publicación del emisor – BMCert Issuing CA:

- AIA: `http://bmcertcrl.managed.entrust.com/AIA/CertsIssuedtoBMCertIssuingCA.p7c`
- CDP: `http://bmcertcrl.managed.entrust.com/CRLs/BMCertIssuingCA.crl`

Con el fin de promover un acceso consistente a Certificados y CRL, el repositorio provee controles de acceso para evitar la modificación o eliminación no autorizada de información. Los directorios de Entrust expuestos a Internet son directorios “cliente” que sólo pueden ser actualizados por los “proveedores” autorizados. Los directorios de los proveedores están protegidos por firewalls y cuentan con controles de acceso que requieren la autenticación positiva de cualquier proceso que intenta escribir o cambiar datos en el directorio.

2.3 Tiempo o Frecuencia de Publicación

CRL: Repositorios para la lista de certificados cancelados.

La frecuencia de publicación de la CRL es una vez cada 6 horas (4 veces al día), con los próximos períodos de actualización programados especificados cada 72 horas.

Repositorio de CP y CPS.

Los cambios de la CPS o CP de la EC, están sujetas a la necesidad de modificación y la respectiva aprobación por parte de la AAC para su puesta en vigencia y publicación respectiva.

2.4 Controles de acceso a los repositorios

Con el fin de promover un acceso consistente a los repositorios indicados en los puntos 2.1 y 2.2, se cuenta con controles de acceso para evitar la modificación o eliminación no autorizada de información. Los directorios de Entrust expuestos a Internet son directorios "cliente" que sólo pueden ser actualizados por los 'proveedores' autorizados. Los directorios de proveedores están protegidos por firewalls y cuentan con controles de acceso que requieren la autenticación positiva de cualquier proceso que intenta escribir o cambiar datos en el directorio.

3.0 IDENTIFICACIÓN Y AUTENTICACIÓN

La EC BMCert utiliza un modelo de registro delegado. En este modelo, ciertos individuos realizan Funciones de Confianza (ERs), son empleados o contratistas de la EC BMCert o socios de negocio actuando como un ER (por ejemplo IOFE-SAC o cualquier otro previamente acreditado ante la AAC). Estos individuos son responsables de la operación de los diversos componentes PKI alojados en las redes de la EC BMCert y socios de negocios.

Además, para la EC BMCert, las ERs son responsables de realizar la identificación y autenticación de las Agencias de Registro o de quien haga sus funciones. La EC BMCert confía en las Entidades de Registro que llevan a cabo la identificación y autenticación para sus suscriptores.

3.1 Nombre

3.1.1 Tipos de nombres

3.1.1.1 Tipos de nombres para la raíz EC

El nombre de la EC Raíz es:

```
cn=BMCERT Root CA, ou=Certification Authorities, o=BMCERT, c=PE
```

3.1.1.2 Tipos de nombres para las raíces intermedias EC

El nombre de publicación de la raiz BMCert es:

```
cn=BMCERT Issuing CA,
ou=Certification Authorities,
o=BMCERT,
c=PE
```

Los tipos del nombre del suscriptor de la raiz BMCert son:

- Función y certificados del usuario (suscriptor):

  ```
  serialNumber=<RUC, DNI>+cn=<Company name>,
  ou=<Certificate type>,
  o=BMCERT, l=<Locality (e.g. Lima)>,
  st=<Province Name>,
  c=<País>,
  ```

  Esta estructura DN se utilizará para emitir certificados a un suscriptor que represente a una organización.

  El RUC es el identificador único de la organización o razón social.

  El DNI es el número del documento de identificación nacional del suscriptor.

  El ou=<Certificate Type> será poblado con:

  - ou=Persona Jurídica; o
  - ou=Agente Automatizado;

  CERTIFICADOS OFRECIDOS

Ítem	Sub - Tipo de certificado	Sujeto (Subject)
Clase I	Autenticación y/o firma digital para persona jurídica	CN (commonName) = <Nombre completo del Titular> SERIALNUMBER = <RUC: Número de RUC de la Organización, DNI: Número del DNI del Suscriptor | CE: Número del carné de extranjería del Suscriptor > O (organization) = <Nombre de la Organización o Razón Social> E (email)= <Correo electrónico> [opcional] L (localityName) = <Provincia de la Organización o Razón Social> S (stateOrProvinceName) = <Departamento de la Organización o Razón Social> C (countryName) = <País de la Organización o Razón Social>
Clase II	Persona Jurídica (Agente Automatizado)	CN (commonName) = <Nombre descriptivo del servidor> SERIALNUMBER = <RUC: Número de RUC de la Organización, SN: Número de serie del servidor> O (organization) = <Nombre de la Organización o Razón Social> E (email)= <Correo electrónico> [opcional] L (localityName) = <Provincia de la Organización o Razón Social> S (stateOrProvinceName) = <Departamento de la Organización o Razón Social> C (countryName) = <País de la Organización o Razón Social>
Clase III	Autenticación y/o firma digital para persona natural	CN (commonName) = <Nombre completo del Titular> SERIALNUMBER = <DNI: Número del DNI del Suscriptor | CE: Número del carné de extranjería del Suscriptor > E (email)= <Correo electrónico> [opcional] L (localityName) = <Provincia de la Organización o Razón Social> S (stateOrProvinceName) = <Departamento de la Organización o Razón Social> C (countryName) = <País de la Organización o Razón Social>
Clase IV	Autenticación y/o firma digital para persona natural con negocio	CN (commonName) = <Nombre completo del Titular> SERIALNUMBER = <RUC: Número de RUC de la Persona Natural, DNI: Número del DNI del Suscriptor | CE: Número del carné de extranjería del Suscriptor > O (organization) = <Nombre completo de la persona natural> E (email)= <Correo electrónico> [opcional] L (localityName) = <Provincia de la Organización o Razón Social> S (stateOrProvinceName) = <Departamento de la Organización o Razón Social> C (countryName) = <País de la Organización o Razón Social>
Clase V	Persona Natural Profesional	CN (commonName) = <Nombre completo del Titular> SERIALNUMBER = <DNI: Número del DNI del Suscriptor | CE: Número del carné de extranjería del Suscriptor > T (title) = <Título Profesional> OU (organizationUnit) = <Siglas del colegio: Número de colegiatura > E (email)= <Correo electrónico> [opcional] L (localityName) = <Provincia de la Organización o Razón Social> S (stateOrProvinceName) = <Departamento de la Organización o Razón Social> C (countryName) = <País de la Organización o Razón Social>

*Las siglas del colegio profesional están contempladas en la tabla adjunta:

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	CLN
Colegio Médico del Perú	CMP
Colegio de Ingenieros del Perú	CIP

3.1.2 Necesidad de que los nombres tengan un significado

Allí donde es utilizada, la cualidad del *commonName* (CN) representa la Organización o Razón Social de una manera que sea significativa. El valor de la cualidad del *commonName* utilizada en el nombramiento de un suscriptor del certificado es significativo. Referirse a la sección 3.1.1.

El nombre del subject tal como se especifica en la EC BMCert coincide con el nombre del emisor de certificados emitidos por la EC BMCert, tal como es requerido por el RFC 5280 (en reemplazo del 3280).

Cuando los dispositivos, aplicaciones y funciones no pueden tener nombres previstos según las normas, la ER se asegura de que un Titular del Certificado del Dispositivo (DCH) posee y es responsable del Certificado en nombre del dispositivo, aplicación o función.

3.1.3 Anonimato o seudónimo de los suscriptores

Se considera válido el uso de seudónimos únicamente en los casos requeridos para identificar a los certificados de los agentes automatizados.

3.1.4 Reglas para interpretar las diferentes modalidades de nombres

Según lo descrito en la sección 3.1.1, en el BMCert PKI sólo se utiliza el formato de nombre DN como el sujeto del certificado en su caso. Esta forma de nombre será interpretado de acuerdo con las normas ISO y aplicables por Internet, tal como se define en el perfil de certificados.

3.1.5 Singularidad 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 resolverá dichas colisiones dentro de su espacio de nombres apropiado. Si la ER no pudiera resolver satisfactoriamente una “colisión de identificadores”, la ER someterá la decisión al Oficial de Seguridad de Información (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.

3.1.6 Reconocimiento, autenticación y rol de las marcas registradas

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.

3.2 Validación inicial de la identidad

3.2.1 Método para probar la posesión de la clave privada

En caso, la clave privada esté asociada a un certificado que se genera en las instalaciones de la ER, éste procedimiento se realizará en presencia del titular o suscriptor del certificado utilizando un medio seguro (p.e. FIPS 140-2 nivel 1), garantizando que en todo momento la clave privada está bajo el control del titular o suscriptor.

En el caso que el certificado digital sea generado directamente por el suscriptor, la solicitud o pedido de certificado debe ser firmado por la clave privada de éste, como prueba de la posesión de la clave privada.

La EC BMCert requiere la prueba de la posesión de la clave privada antes de crear y de firmar un certificado que contiene la clave pública asociada. La prueba de la posesión de una clave privada es manejada por dos métodos primarios siguientes:

- Usando infraestructura de clave pública (X.509) - protocolo de gestión de certificado (PKIX-CMP); como tal, cualquier transmisión electrónica será protegida; o
- Utilizando PKCS#10 de las solicitudes de certificado de firma. La solicitud inicial debe ser firmada por la clave privada correspondiente a la clave pública contenida en la solicitud, lo que demuestra la posesión de la clave privada.

Otros métodos aceptables incluyen la firma de tokens de desafío-respuesta, y el empleo de la clave privada correspondiente al uso en canales seguros de comunicación.

3.2.2 Autenticación de la Identidad de una persona jurídica

La entidad Raíz EC BMCert (BMCert Root CA) no emitirá directamente certificados de organización (Certificados en la que el Sujeto del Certificado representa una organización o grupo, en lugar de un individuo o dispositivo específico), con excepción de la EC BMCert intermedia . Los certificados emitidos por la EC Raíz para otras EC se emitirán de acuerdo con los requisitos definidos en esta CPS. Todas las solicitudes de certificados de otras EC on-line incluirán información de identidad del representante de la organización solicitante que se remitirá al Oficial de Seguridad para su aprobación.

La EC BMCert intermediaria (BMCert Issuing CA) emitirá certificados on-line de la organización, excepto para otras CA Intermedias. La ER verificará en todas las solicitudes la existencia de una organización consultando que en la base de datos de la SUNAT, la entidad se encuentre en estado "activo" y que la condición de su domicilio sea "habido".

La ER deberá mantener un registro de los medios utilizados para establecer la identidad de la organización y de la persona autorizada para actuar en nombre de la organización, y cualquier tipo de identificación utilizada, y deberá mantener una copia de la evidencia de la identificación por diez (10 años).

3.2.3. Autenticación de la Identidad individual

La validación de la identidad de los representantes legales o titulares del certificado de Persona Jurídica o Agente Automatizado (suscriptores), según el procedimiento de trámite de emisión y entrega del certificado digital, se podrá realizar de la siguiente manera:

- Para el caso de los ciudadanos peruanos, la ER hará la validación de la identidad del solicitante, la cual consite en verificar y/o autenticar su identidad empleando la base de datos del RENIEC y/o su Documento Nacional de Identidad – DNI.
- Para el caso de los extranjeros, la ER hará la comprobación de la identidad del solicitante, la cual consiste en verificar y/o autenticar su identidad consultando al sistema de Migraciones.

3.2.4 Información no verificada del suscriptor

La información que no se verifica no se incluirá en los Certificados.

3.2.5 Validación de la autoridad

Antes de generar los certificados de la EC BMCert que establecen la autoridad de la organización, la ER debe validar la facultad de la persona para actuar en nombre de la organización. El solicitante es responsable de presentar los documentos requeridos a la ER. La ER debe validar los datos de acuerdo con su Declaración de Prácticas de Registro.

3.2.6 Criterios para la Interoperabilidad

El Oficial de Seguridad de BMCert determinará los criterios de interoperabilidad para las entidades emisoras (certificado cruzado) que operan bajo este documento.

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

La EC BMCert no brindará servicio de re-emisión de certificados digitales.

3.3.1. Identificación y autenticación para solicitudes de re-emisión de certificado rutinaria

La EC BMCert no brindará servicio de re-emisión de certificados digitales.

3.3.2. Identificación y autenticación para solicitudes de re-emisión de certificado luego de la revocación

La EC BMCert no brindará servicio de re-emisión de certificados digitales.

3.4 Identificación y autenticación de la solicitud de revocación

La ER deberá validar la identidad del solicitante antes de proceder con la revocación del certificado digital a través del MSO de la EC BMCert.

Los solicitantes de revocación de un Certificado digital pueden ser el Suscriptor o Titular del certificado digital autenticadas mediante una Pregunta y Respuesta (Q & A) registrada por el Suscriptor con la solicitud de la ER durante el proceso de inscripción.

Detalles adicionales pueden ser provistos en la DPR de la ER.

4.0 REQUISITOS OPERACIONALES DEL CICLO DE VIDA DE LOS CERTIFICADOS

Los procesos del ciclo de vida de un certificado digital de la EC BMCert para persona jurídica se encuentran establecidos en: bmcert.pe/documentos.

4.1 Solicitud del certificado

El solicitante (Persona Jurídica) que desee gestionar un proceso de solicitud de certificado, deberá apersonarse a una oficina de la ER que tenga convenio con EC BMCert y proporcionar la información suficiente para:

- Establecer la autorización del Solicitante (representante/apoderado de la persona jurídica) para obtener un certificado digital (según la sección 3.2.3);
- Establecer y registrar la identidad del solicitante (según la sección 3.2.3);
- Obtener la clave pública del Solicitante y verificar que el Solicitante tenga la clave privada para cada certificado requerido (según la sección 3.2.1); y
- Verificar cualquier papel/rol o información de autorización solicitada para su inclusión en el certificado digital.

Todos los pasos anteriores se completan antes de la emisión del Certificado. Antes de la primera emisión de certificados digitales, todos los usuarios de la ER correspondiente se deberán autenticar a la EC BMCert y proporcionar la identificación requerida, como se especifica en la Sección 3.2.3.

Todo los Oficiales de Seguridad (excepto el primer oficial del MSO Entrust) y de la ER, utilizan cualquiera de las tarjetas inteligentes u otros tokens criptográficos para la generación y almacenamiento de sus claves privadas.

En caso la ER requiera un certificado con información adicional, deberá solicitarlo a la EC BMCert, la ER deberá verificar la información brindada por el solicitante antes de incluirla en el certificado digital (por ejemplo RENIEC y SUNARP).

Los detalles relativos al proceso de emisión de certificados se encuentran en la Sección 4.3 y en la DPR de la EC BMCert.

4.1.1 Habilitados para presentar la solicitud de un 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. Para estos certificados digitales, el titular es la persona jurídica y los suscriptores son las personas naturales autorizadas por el representante del titular para solicitar un certificado digital.

4.1.2 Proceso de solicitud y responsabilidades

Todas las comunicaciones de la EC BMCert, que soportan la solicitud de certificado digital y el proceso de emisión son autenticadas y protegidas contra modificaciones; cualquier transmisión electrónica de los secretos compartidos está protegido. La comunicación electrónica entre los entornos de inscripción de la EC BMCert están cifrados y firmados digitalmente.

4.2 Procesamiento de la solicitud de Certificado

La información en las solicitudes de certificado se verifican como exactas antes de que se emitan los certificados digitales. La verificación a realizar depende del nivel de seguridad en el que se está acreditando la EC BMCert, que en este caso es Nivel Medio.

En la sección 3.2.3. de esta CPS se tiene mayor información al respecto.

4.2.1 Realización de funciones de Identificación y Autenticación

La identificación y la autenticación del suscriptor cumple con los requisitos especificados para la autenticación del suscriptor especificada en la sección 3.2 de la presente CPS. La sección 3.2.3 de la presente CPS identifica los componentes (por ejemplo Agencias de Registro) que son responsables de la verificación de la identidad del suscriptor en cada caso.

4.2.2 Aprobación o Rechazo de la solicitud de emisión de un certificado

El solicitante (Persona Jurídica) 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. El solicitante debe entregar la información solicitada por la ER y asume la responsabilidad por la veracidad y exactitud de la información proporcionada, sin perjuício de la respectiva comprobación por parte de la ER, la cual debe estar debidamente acreditada.

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 implementando 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, asi 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 DPR 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 (específica o general) 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 el procesamiento de la solicitud de un 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 dias útiles, a través de un proceso automático.

4.3 Genenración de Claves y Emisión del Certificado

Una vez que el Registrador(es), autentica la identidad del suscriptor y verifica la elegibilidad del suscriptor para recibir un Certificado (ver secciones 3.1 y 4.1), el Registrador(es) utiliza una aplicación web, XAP o aplicación PKIX-CMP para autorizar la emisión de un certificado al suscriptor.

4.3.1 Acciones de la EC durante la emisión del certificado

Cuando reciba una solicitud, la ER debe:

- Verificar la identidad del solicitante (más detalles en la sección 3.2.3);
- Verificar la autoridad del solicitante y la integridad de la información en la solicitud del certificado (sección 3.2.1);
- Realizar la recepción del pedido de certificado (request) firmado con la clave privada recién

generada del suscriptor.

- Proteger la confidencialidad e integridad de los datos del solicitante del certificado.
- Publicar en el repositorio el certificado emitido, utilizando los controles establecidos para garantizar la seguridad de la información.
- Almacenar de forma automática en los registros de la EC, la fecha y hora en la que se expidió el certificado.

4.3.2 Notificación al suscriptor por parte de la EC respecto de la emisión de un certificado

Como se indica en el apartado 4.3.1, cada suscriptor participa activamente con la emisión de sus certificados. En caso de presentarse inconvenientes en este paso, el suscriptor deberá comunicarse con la Entidad de Registro o la Agencia de Registro correspondiente o al Centro de Contacto que se muestra en la página WEB de la EC BMCert:

https://bmtech.pe/documentos

4.4 Aceptación del Certificado

Antes de que un suscriptor pueda hacer un uso efectivo de su clave privada, la ER deberá:

- Informar al suscriptor sus responsabilidades tal como se definen en el presente documento; e
- Informar al suscriptor de la creación de un certificado y el contenido del certificado.

4.4.1 Conducta constitutiva de la aceptación de un certificado

El Contrato firmado por el suscriptor garantiza el reconocimiento y acuerdo con los términos y condiciones contenidos del presente documento que rigen los derechos y obligaciones de la ER, EC y del suscriptor, además de reconocer la presente Declaración de Prácticas y Políticas de Certificación, que rige técnica y operativamente los servicios de certificación digital prestados por la EC BMCert.

LA ACEPTACIÓN DEL CERTIFICADO POR EL SUSCRIPTOR INDICARÁ EL ACUERDO CON EL SUSCRIPTOR PARA CUMPLIR CON TODAS LAS DISPOSICIONES DESCRITAS EN ESTA POLÍTICA Y TODAS LAS OBLIGACIONES ASOCIADAS CON EL USO DEL CERTIFICADO.

La EC BMCert puede imponer requisitos adicionales que no están incluidos en el presente documento, en caso afirmativo el suscriptor será informado de estos requisitos.

4.4.2 Publicación del certificado por parte de la EC

La información concerniente a los certificados digitales emitidos será publicada en el Repositorio de la EC BMCert.

4.4.3 Notificación de la EC a otras entidades repecto a la emisión de un certificado

La EC BMCert (EC BMCert Issuing) no emitirá certificados de la EC a otras Entidades Certificadoras.

4.5 Par de Claves y Uso del Certificado

4.5.1 Uso de la clave privada y certificado por parte del suscriptor

El alcance previsto de la utilización de una clave privada se especifica a través de las extensiones del certificado, incluyendo el uso de claves y las extensiones de uso de clave extendida 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 la clave pública y el certificado por el tercero que confía

La política de emisión de la EC BMCert del certificado, especifica restricciones de uso a través de las extensiones críticas de los certificados, incluidas las restricciones básicas y las extensiones de uso de claves. La PKI emite la CRL que especifica el estado actual de todos los certificados no expirados.

La AAC permite al tercero que confía el acceso a los certificados publicados en el Repositorio con las restricciones incluidas en el presente documento.

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).

Más información a través de la página de la EC BMCert (bmtech.pe).

4.6 Renovación del Certificado

No aplica.

4.6.1 Circunstancias para la re-certificación de los certificados (renovación de certificados con el mismo par de claves)

No aplica.

4.6.2 Personas habilitadas para solicitar la renovación

No aplica.

4.6.3 Procesamiento de la solicitud de renovación de certificado

No aplica.

4.6.4 Notificación al suscriptor respecto a la emisión de un nuevo certificado

No aplica.

4.6.5 Conducta constitutiva de aceptación de renovación de un certificado

No aplica.

4.6.6 Publicación de la renovación por parte de la EC de un certificado

No aplica.

4.6.7 Notificación de la EC a otras entidades respecto a la renovación del certificado

No aplica.

4.7 Re-Emisión de Certificado

No aplica.

4.7.1 Circunstancias para la re-emisión de un certificado

No aplica.

4.7.2 Personas habilitadas para solicitar la re-emisión de certificado

No aplica.

4.7.3 Procesamiento de las solicitudes para re-emisión de certificados

No aplica.

4.7.4 Notificación al suscriptor sobre la re-emisión de un certificado

No aplica.

4.7.5 Conducta constitutiva de la aceptación de una re-emisión de certificado

No aplica.

4.7.6 Publicación por parte de la EC del certificado re-emitido

No aplica.

4.7.7 Notificación por parte de la EC a otras entidades respecto a la reemisión de certificados

No aplica.

4.8 Modificación del Certificado

No aplica.

4.8.1 Circunstancia para la modificación de un certificado

No aplica.

4.8.2 Personas habilitadas para solicitar la modificación de un certificado

No aplica.

4.8.3 Procesamiento de las solicitudes de modificación de certificados

No aplica.

4.8.4 Notificación al suscriptor sobre la emisión de un nuevo certificado

No aplica.

4.8.5 Conducta constitutiva de la aceptación de un certificado modificado

No aplica.

4.8.6 Publicación por parte de la EC del certificado modificado

No aplica.

4.8.7 Notificación por parte de la EC a otras entidades respecto a la emisión de certificados modificados

No aplica.

4.9 Revocación y Suspensión del Certificado

4.9.1 Circunstancias para la revocación

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

- Se pierde, se roba, o se compromete la clave privada del suscriptor;
- Por deterioro, alteración o cualquier otro hecho u acto que afecte la clave privada.
- Por revocación de las facultades de representación y/o poderes de sus representantes legales o apoderados.
- El suscriptor ya no está afiliado con la operación o el mantenimiento de la EC BMCert;
- El suscriptor deja de laborar en Entrust o BMCert;
- La información de identificación del suscriptor contenida en el certificado no es más válida;
- El suscriptor se olvida la contraseña y no es posible la recuperación;
- El suscriptor u otra parte autorizada pide que el certificado del suscriptor sea revocado;
- El suscriptor que representa a una organización (por ejemplo, Persona Juridica) ya no representa a esta organización.
- Cuando el suscriptor o titular incumple las obligaciones a las que se encuentra comprometido dentro de la IOFE a través de lo estipulado en el contrato del suscriptor y/o titular.
- Cuando la información contenida en el certificado ya no resulte correcta.
- Por adecuacuón a la legislación respectiva.

4.9.2 Personas habilitadas para solicitar la revocación

Se encontrarán habilitadas para solicitar la revocación de un certificado digital en las circunstancias señaladas en la sub sección 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 para la solicitud de revocación

Cuando alguna de las circunstancias en la Sección 4.9.1 se producen, la ER que recibe la solicitud de revocación debe procesar la solicitud tan pronto como sea posible después de recibir la solicitud.

La EC BMCert aceptará el pedido de revocación del certificado digital realizada por la ER que aprobó su emisión, el pedido de revocación debe ser autorizado por ésta y enviado únicamente mediante canales seguros, de la siguiente manera:

1. Autenticar la solicitud de revocación, como se ha definido en la sección 3.4 de este CPS y DPR;
2. Establecer una conexión segura al servidor de la EC;
3. Autenticarse en el servidor de la EC utilizando sus credenciales PKI;
4. Utilizar el software/canal de administración de la ER para indicar que el certificado fue revocado; y
5. Verificar que el servidor de la EC complete el proceso de revocación.

4.9.4 Periodo 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. Todas las solicitudes de revocación de certificados se hacen, como se indica en las secciones 4.9.1 - 4.9.3, inmediatamente después de la indicación de que se ha producido alguna de las circunstancias señaladas en la Sección 4.9.1.

4.9.5 Tiempo dentro del cual una 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 indicado por la ER. Las solicitudes de revocación se procesan antes de que se publique la CRL siguiente. Las solicitudes de revocación se procesan en función del mejor esfuerzo.

4.9.6 Requerimientos para la verificación de la revocación de certificados por los terceros 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 la emisión de CRL

La frecuencia de la emisión de CRL se expedirá de forma programada, una vez cada 6 horas (4 veces al día), con los próximos períodos de actualización programados especificados cada 72 horas, incluso si no hay cambios a realizar, para asegurar la puntualidad de la información. La información del estado del certificado puede ser emitida con mayor frecuencia que la frecuencia de emisión que se describe a continuación.

La EC BMCert brinda el servicio de CRL, con una disponibilidad mínima del 99% anual y con un tiempo programado de inactividad máximo de 0.5% anual.

4.9.8 Máxima Latencia para CRLs

Las CRLs se publican dentro de las 4 horas siguientes de su generación. Además, cada CRL se publica a más tardar el tiempo especificado en el campo *nextUpdate* de la CRL emitida anteriormente para el mismo alcance.

4.9.9 Disponibilidad de la verificación en línea de la revocación/estado

No aplica.

4.9.10 Requisitos para la verificación en línea de la Revocación

No aplica.

4.9.11 Otras formas disponibles de publicar la revocación

No aplica.

4.9.12 Requisitos especiales para el caso de compromiso de la clave privada

Cuando un certificado de suscriptor es revocado por estar comprometido o se sospecha el 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 de esa caché CRL.

Si una EC debe ser revocada, BMCert debe comunicarse inmediatamente con Entrust para remediar la situación y revocar la EC si fuera necesario. Una vez que el Oficial de Seguridad del MSO (Entrust) aprueba la revocación de la EC, se dará por terminada. Salvo para el caso de las EC off-line.

4.9.13 Circunstancias para la suspensión

No aplica.

4.9.14 Personas habilitadas para solicitar la suspensión

No aplica.

4.9.15 Procedimiento para solicitar la suspensión

No aplica.

4.9.16 Límite del periodo de suspensión

No aplica.

4.10 Servicios de estado de certificado

No aplica.

4.10.1 Características operacionales

No aplica.

4.10.2 Disponibilidad del servicio

No aplica.

4.10.3 Rasgos operacionales

No aplica.

4.11 Finalización 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 ítem 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 DPR.

4.12 Depósito y recuperación de claves

4.12.1 Políticas y prácticas de recuperación de Depósitos de claves

Las claves privadas no deben se custodiadas por la EC BMCert.

La EC BMCert no emite certificado de cifrado.

La EC BMCert no custodia las llaves usadas para la firma digital o el non-repudiation. Ninguna parte externa está autorizada a mantener un fideicomiso de llaves asociadas con Certificados emitidos por la EC BMCert.

4.12.2 Políticas y prácticas para la encapsulación de claves de sesión

No Aplica.

5.0 CONTROLES DE LAS INSTALACIONES, DE LA GESTION Y CONTROLES OPERACIONALES

La información contenida en esta sección es específica para la gestión de instalaciones y controles operativos ejecutados por la EC BMCert para soportar su infraestructura en la premisa de la ER.

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 del 5.1.1 al 5.1.8. Dichos equipos están protegidos contra el robo, la pérdida y el uso no autorizado, según la ISO/IEC 27001 (Information technology - Security techniques - Information security management systems – Requirements)

5.1.1 Ubicación y construcción del local

La infraestructura para servicios de la EC BMCert se encuentra dentro de la instalación de Entrust en Ottawa, Canadá. Los equipos que componen el PKI de la EC BMCert se encuentra en una zona de seguridad que está físicamente separada de otros sistemas de Entrust para que sólo el personal autorizado de la EC BMCert pueda acceder a él. La zona de seguridad se construye mediante paredes, piso y techo de concreto con paneles de yeso y malla de alambre. La zona de seguridad está protegida por sistemas de control electrónico de acceso/niveles, puertas con alarma y monitoreo mediante una cámara de seguridad y un sistema de detección de movimiento registrados 24x7. Las instalaciones no se encuentran en zonas geográficas propensas a los desastres naturales (por ejemplo, terremotos,

inundaciones).

Estas instalaciones se constituyen de múltiples capas de acceso físico para proteger los sistemas que soportan el PKI de la EC BMCert.

5.1.2 Acceso físico

El acceso físico a las aplicaciones de la EC BMCert se protege usando los controles de Entrust, la sala que contiene el software de PKI de la EC BMCert está designada para la presencia de almenos (2) personas, y los controles son utilizados para evitar que una persona esté sola en la habitación.

Las instalaciones cuentan con detectores de presencia para notificar al personal de seguridad de cualquier violación de las reglas para el acceso físico.

5.1.3 Energía y aire acondicionado

La zona de seguridad está equipada con:

- La energía es filtrada, se emplean estabilizadores de corriente conectados a un UPS y el generador de energía es de la capacidad adecuada;
- Calefacción, ventilación y aire acondicionado apropiados para en las salas que albergan los equipos informaticos que componen el sistema PKI de la EC BMCert; y
- Iluminación de emergencia.

Los controles de ambientes se ajustan a las normas locales y están adecuadamente asegurados para evitar el acceso no autorizado y/o manipulación del equipo. Las alarmas y alertas de control de temperatura se activan al detectar condiciones de temperatura amenazantes.

5.1.4 Exposición al agua

Las instalaciones de toda la infraestructura de servicios de la EC BMCert cuenta con proteción contra exposiciones al agua. No hay tuberías de líquido, gas, escape, etc. que atraviesen el espacio controlado que no sean las directamente necesarias para el sistema HVAC y para el sistema de pre-acción a extinción de incendios. Los tubos de agua para el sistema de pre-acción de supresión de incendio sólo se llenan en la activación de múltiples alarmas de incendio.

5.1.5 Prevención y protección contra fuegos

Las instalaciones de Entrust que alojan la infraestructura de la EC BMCert está completamente cableada para detección de incendios, alarma y supresión. Se realizan inspecciones rutinarias y frecuentes de todos los sistemas para asegurar un funcionamiento adecuado.

5.1.6 Archivo de material

Todos los medios que necesitan ser protegidos (por ejemplo, registros de papel, CDs, etc.) se almacenan en un contenedor de almacenamiento a prueba de fuego y agua. Los medios electromagnéticos también se almacenan en el contenedor. El contenedor se puede bloquear y se mantiene en un entorno de control

de acceso, lo que protege de los medios contra el acceso no autorizado. El material archivado se almacena en la instalación de almacenamiento de archivos aprobada por la EC BMCert.

5.1.7 Gestión de residuos

Los residuos de papel que contienen información sensible se depositan en un contenedor de eliminación cerrado en las instalaciones del PKI de la EC BMCert (Entrust). Cuando el contenedor está lleno, el contratista especializado en la eliminación de documentos sensibles está programado para recoger y destrozar el material.

Los medios que contienen información sensible en forma electrónica se sobrescriben con el software de seguridad aprobado por la EC BMCert, desmagnetizado, desmenuzado y/o quemado antes de su eliminación.

5.1.8 Copia de seguridad externa

Los servicios de copia de seguridad son proporcionados por Entrust.

Las copias de seguridad se realizan diariamente y los datos del sitio principal se transfieren electrónicamente al sitio de copia de seguridad. El sitio de copia de seguridad tiene controles físicos y de procedimiento equivalentes en su lugar como el sitio principal. Las copias son establecidas y mantenidas en conformidad con las políticas de archivo y continuidad del negocio y el plan de recuperación frente a desastres cumpliendo los estándares del ISO.

5.2 Controles Procesales

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:

1. ER (ejemplo. ER IOFE SAC)

Los empleados, consultores y contratistas designados a gestionar la infraestructura de confianza son clasificados como “personas de confianza” sirviendo en “roles de confianza”. Los roles de confianza también deben incluir, al menos los dichos roles que contemplen las siguientes responsabilidades:

- Responsabilidad general para administrar la implementación de prácticas de seguridad de la EC;
- Aprobación de la generación, y revocaciónde los certificados;
- Configuración y mantenimiento de la infraestructura de la EC;
- Operaciones rutinárias de los sistemas de la EC, respaldo y/o recuperación de sistemas;
- Auditoría interna para ejecutar la inspección y mantenimiento de los expedientes de la infraestructura de la EC y registros de auditoría;
- Gestión del ciclo de vida de claves criptográficas;

El Oficial de Seguridad de BMCert es responsable de identificar a quienes puedan cumplir el rol de la ER en el marco de la Infraestructura Oficial de Firma Electrónica.

La ER es responsable de realizar la gestión del ciclo de vida del usuario para todos los suscriptores que participan en la PKI. La ER es responsable de realizar la identificación y autenticación de los suscriptores; emisión y revocación de certificados emitidos a los suscriptores; Y mantenimiento de la documentación completa que demuestre el cumplimiento del presente documento en su referido rol.

5.2.2 Número de personas requeridas por labor

Todas las operaciones de las ERs con las que la EC BMCert tiene convenio, garantizan al menos dos personas en la ejecución de las tareas de la EC BMCert

Las siguientes operaciones necesitan de dos autorizaciones de la EC BMCert con la ER que tiene convenio:

- Añadir suscriptores
- Revocación de suscriptores
- Manipulación del dispositivo de custodia de las claves de EC BMCert Root y la EC BMCert Issuing.

5.2.3 Identificación y autenticación para cada rol

Un usuario se identifica y se autentica antes de que se le permita realizar cualquier acción establecida anteriormente para esa función o identidad. Los suscriptores que cumplen las funciones de confianza y que han recibido credenciales de la EC BMCert (por ejemplo, ER) se autentican en el sistema de la EC con credenciales PKI almacenadas en un módulo de hardware criptográfico aprobado.

5.2.4 Roles que requieren funciones por separado

Todas las funciones de los roles requieren separación de los deberes e incluye (pero sin limitación) a los designados de ejecutar los siguientes roles:

- Validación de la información en aplicaciones de certificado y de solicitudes o información del suscriptor.
- Aceptación, rechazo, de la solicitud del certificado, solicitud de revocación, información de afiliación.
- Emisión, o revocación de los certificados, incluyendo personal con acceso limitado del repositorio de certificados.
- Generación, emisión o destrucción de los certificados.
- Auditoría

5.3 Controles de Personal

5.3.1 Cualidades y requisitos, experiencia y certificados

Para la EC BMCert y la ER con la cual la EC BMCert tiene convenio, así como sus Business Partners se seleccionan basándose en la lealtad, fiabilidad e integridad. Todos los individuos que llenan estos roles deben cumplir con los siguientes requisitos, antes de tener acceso físico o lógico a la solicitud de la EC BMCert de acuerdo a la "Norma Marco sobre privacidad de APEC" (anexo 6 de la Guía de Acreditación para Entidades de Certificación Digital y Entidades Conexas):

- Para la EC BMCert, será algún empleado de la misma o empleado del contratista de la EC BMCert;
- Para la ER con la cual se celebra convenio, será un empleado de la misma ER o empleado del contratista de esta ER; y
- Será nombrado por escrito como miembro conforme a la política de la EC BMCert o delegado Representante del Socio Comercial (BMCert).

Las copias de la documentación que demuestren que los individuos llenan los roles de confianza para la PKI, mientras cumplen estos requisitos serán mantenidos por política de la EC BMCert y serán realizados por su representante de socios comerciales y serán puestos a disposición durante las auditorías de cumplimiento.

Además de lo anterior, los individuos que llenan roles de confianza para la PKI:

- No han sido previamente relevados de los deberes o responsabilidades del PKI por motivos de negligencia o incumplimiento de sus deberes;
- No han sido condenados por un delito grave;
- Han completado exitosamente un programa de entrenamiento apropiado; y
- Han demostrado la capacidad de desempeñar sus funciones.

5.3.2 Procedimiento para la verificación de antecedentes

Los controles a los antecedentes se llevarán a cabo como parte del proceso de selección del personal del socio de negocios de la ER IOFE SAC y/o cualquier otra ER acreditada.

El agente de registro de la ER IOFE SAC ejecuta los controles mínimos como:

- Recopila los documentos de la empresa como son: Copia de la Ficha RUC de la empresa; Copia literal actualizada de la empresa; Copias de los documentos de identidad; Vigencia de poder del representante legal.(mínimo 01 mes de antigüedad)
- Se realiza el estudio de poderes, a cargo de un estudio de abogados, quienes cuentan con las herramientas de verificación de la identidad de estas personas, mediante la consulta efectuada a la Base de Datos del Registro Nacional de Identificación y Estado Civil (RENIEC) y los poderes que dice tener en la empresa en la Base de Datos dela SUNARP.
- Verificación de cualidades y referencias, el día de la entrega del certificado, de manera presencial o por videoconferencia con las personas consignadas en las referencias de la solicitud

presentada a nuestra ER.

Si se cuestiona la confiabilidad de un individuo que llena un rol de confianza, el individuo será removido de la posición delicada 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 capacitación

Todo el personal que desarrolla funciones con respecto al funcionamiento de las aplicaciones de ER reciben una formación integral. La capacitación se lleva a cabo en las siguientes áreas:

- Principios y mecanismos de seguridad de la ER;
- Todas las versiones de software PKI en uso en el sistema de la ER;
- Uso/operación del hardware y software empleado.
- 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.
- Tareas en relación al Plan de Contingencias, operación, administración y seguridad para cada rol epecífico de la ER.

Se establecen los requisitos de formación para cada rol de confianza para la PKI, incluida la formación en la realización de las funciones de la función específica y la formación de PKI en general.

El personal que se ha sido asignado a un rol de confianza no comienza a trabajar en ese rol sin supervisión hasta que haya recibido la formación para ese rol y la experiencia documentada equivalente puede ser sustituida por la formación necesaria para un individuo a discreción del Oficial de Seguridad de la EC BMCert.

Los registros de capacitación para todo el personal que realizan roles de confianza serán mantenidos por la EC BMCert o su representante y socio de negocios y estarán a disposición de los auditores durante cada auditoría de cumplimiento.

5.3.4 Frecuencia y requisitos de las re-capacitaciones

Todas las personas responsables de roles de confianza son conscientes de los cambios en la operación ER. Cualquier cambio significativo, (determinado por la EC BMCert en el tiempo, por ejemplo las que incluirán cambios en los procedimientos, cambios en la configuración de PKI o la arquitectura, etc.) a este CPS, DPR, hardware PKI, o software requiere actualización y capacitación del personal afectado. El programa de capacitación Rol de confianza abarca los principios y mecanismos de seguridad (incluyendo una sesión práctica con el software de la ER) y funciones de PKI. Los procedimientos de operaciones se documentan y se actualizan cuando hay un cambio en los procedimientos. La política de la EC BMCert determinará cuando se requiere la capacitación y/o re-asignación de las personas que realizan funciones de confianza para la PKI, y se le proporcionará toda la reconversión necesaria.

Los registros de capacitación para las personas que cumplen los roles de confianza son mantenidos por el Oficial de Seguridad de BMCert o su representante socio de negocios (ER).

5.3.5 Frecuencia y secuencia de la rotación en el trabajo

No aplica.

5.3.6 Sanciones por acciones no autorizadas

Cualquier persona de la EC BMCert o sus socios comerciales que actúen en violación de las prácticas y procedimientos establecidos en el presente documento, ya sea por negligencia o con mala intención, pueden ser condición y privilegios revocados y pueden ser objeto de medidas administrativas y disciplinarias. Reiterada la violación significativa de la política puede resultar en una o más de las siguientes acciones: la eliminación de un rol de confianza, la terminación del empleo y el enjuiciamiento (sujeto a las limitaciones de la EC BMCert y contratos de trabajo Business Partner).

5.3.7 Requisitos de los contratistas

Todo el personal contratado en su rol de confianza cumple con los mismos requisitos que los no contratados que realizan roles de confianza. Todos los contratistas tendrán que firmar un formulario de acuerdo de suscriptor PKI. Estos requisitos se definen en el ítem 5.3 del presente documento. El Oficial de Seguridad de la EC BMCert, o su delegado, es responsable de asegurar que únicamente los contratistas que cumplan estos requisitos se colocan en los roles de confianza para la EC BMCert.

5.3.8 Documentación suministrada al personal

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

Como mínimo, la siguiente documentación estará disponible según lo requiera cada Rol de Confianza de la EC BMCert:

1. BMCert CP;
2. BMCert CPS; y
3. DPR de la EC BMCert.

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 sus roles para la ejecución de sus labores.

Según la Sección 5.3.3, del presente documento, se mantienen registros de capacitación de la EC BMCert que muestran cuándo y qué fue recibido en la capacitación interna. Para la capacitación externa pertinente a las obligaciones de la EC BMCert, se mantendrán copias de los certificados.

5.4 Procedimientos de Registro de Auditorías

Todos los acontecimientos de seguridad, los materiales utilizados y acciones ejecutadas por la ER en el sistema de la EC automáticamente se registran en archivos históricos de auditoría.

Como especificado en el presente documento, hay otros eventos auditables que no pueden ser capturados en registros de auditoría electrónicos.

5.4.1 Tipos de eventos registrados

Además de lo que ya está estipulado en este documento, BMCert y sus socios comerciales que actúan como una ER pueden registrar los siguientes tipos de eventos del ciclo de vida de certificados generados por las aplicaciones de ER:

- Solicitudes de certificados;
- Verificación de las solicitudes de certificados;
- Renovación y cambio de claves del certificado y solicitudes; y
- Solicitudes de revocación
- Encendido y apagado de los sistemas.
- Intentos de crear, borrar, cambiar contraseñas o permisos de los usuarios dentro del sistema de certificación.
- Intentos de entrada y salida del sistema de certificación.
- Intentos no autorizados de acceso a los registros o bases de datos del sistema de certificación.
- Cambios en las políticas de emisión de certificados.
- Intentos no autorizados de entrada a la red de la EC.
- Generación de claves de la EC.
- Intentos nulos de lectura y escritura en un certificado y en el repositorio.
- Eventos relacionados con el ciclo de vida del certificado: emisión, revocación.

El registro de auditoría de eventos registra la hora, fecha y software/hardware utilizados.
La EC registrará de manera manual o electrónica, la siguiente información:

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

5.4.2 Frecuencia del procesamiento del Registro

Además de lo que ya está estipulado en el presente documento el Oficial de Seguridad de BMCert o su delegado revisa manualmente los registros de auditoría.

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. Los resúmenes del registro de auditoría se envían al Oficial de Seguridad de BMCert al final de cada revisión. Las acciones tomadas como resultado de

estas revisiones se documentarán actualizando la documentación de operaciones o con una solicitud de cambio de configuración.

5.4.3 Período de conservación del Registro de Auditorías

Los datos del registro de auditoría generados por las aplicaciones ER se mantienen en vivo en el hardware por un mínimo de un mes. Los registros se copian (no se eliminan) de los servidores de aplicaciones ER a un sitio de Recuperación de Desastres diariamente.

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

5.4.4 Protección del registro de Auditoría

Tanto físicos como electrónicos, los registros de auditorías cuentan con medidas de protección física y lógica, como:

- Lista de control de acceso a lectura.
- Protección contra modificaciones.
- Luego de transcurrido el plazo de diez (10) años de mantenimiento del registro de auditoría su destrucción sólo se podrá llevar a cabo con la autorización de la AAC.

5.4.5 Procedimiento de copia de seguridad del registro de auditorias

Los registros de auditoría de seguridad son generados como mínimo de manera mensual y contienen una copia de seguridad del registro de auditorías y de las aplicaciones de la ER, la cual es archivada fuera de sus instalciones, de acuerdo con los procedimientos de copia de seguridad de la EC BMCert y sus asociados de negocios.

5.4.6 Sistema de realización de Auditoría (Interna vs Externa)

- La frecuencia de las auditorías internas de la EC BMCert se realiza una vez cada seis (6) meses.
- La frecuencia de las auditorías externas de la EC BMCert se realiza una vez al año (auditoría periódica).
- Las auditorías externas pueden también ser llevadas a cabo siempre que la AAC lo requiera (auditoría extraordinaria).

5.4.7 Notificación al titular que causa un evento

Los suscriptores de la EC BMCert que causan los eventos de auditoría reciben la notificación, según el caso, a través del Software de Entrust, BMCert y el su socio de negocios.

5.4.8 Valoración de vulnerabilidad

La EC BMCert a través de los servicios de Entrust cuenta con hardware y software que cumplen con altos estándares de seguridad, tales como:

- CC EAL4+ (ISO/IEC 15408), NIAP PP CIMC SL3
- FIPS 140-2 nivel 3

- ISO 27001: 2013
- ISO 21188
- HSPD-12 APPROVED PRODUCT LIST
- GSA (General Services Administration)
- SSAE-16

Además es responsabilidad del personal de la EC BMCert informar al Oficial de Seguridad cualquier tipo de evento que pueda producir (o potencialmente producir) alguna vulnerabilidad en el hardware o software de la EC BMCert

5.5 Archivo de Registros

BMCert y sus socios de negocio que actúan como un ER no archivan datos, pero mantienen los archivos de registro de aplicaciones ER con la premisa de mantenerlo en medios de copia de seguridad durante un período de 10 años.

5.5.1 Tipos de eventos registrados

BMCert registra los eventos generados por la ER en las instalaciones y sistemas implicados en la gestión de certificados. Los registros de auditoría se generan mediante los siguientes eventos:

- Detalles/datos del certificado digital como Número de serie, estado e información del suscriptor.
- Lista de Certificados digitales cancelados.
- Claves públicas de la EC.
- Estado de acreditación de la EC.
- Registros de auditorías.

La EC BMCert es responsable del correcto archivamiento de estos registros.

5.5.2 Periodo de conservación del archivo

La EC BMCert y sus socios de negocios no archivan datos, pero mantienen vigente los archivos en los medios de copia de seguridad por un período de 10 años.

5.5.3 Protección del archivo

Los archivos de registro son protegidos físicamente lógicamente y supervisados para evitar el uso inadecuado.

5.5.4 Procedimientos para copia de seguridad del archivo

La EC BMCert mantiene la integridad y disponibilidad de los servicios de procesamiento de información y comunicaciones, realizando copias de seguridad, tanto de la información como del software primordial para el funcionamiento de la EC. Estas copias son probadas con regularidad por el personal autorizado.

5.5.5 Requisitos para los archivos de sellado de tiempo

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 del archivo (interna o externa)

Los datos de registro de la ER se recogen como parte de los procedimientos rutinarios del respaldo de sistema.

5.5.7 Procedimiento para obtener y verificar la información del archivo

Dependiendo de la naturaleza de la información contenida en el archivo, el acceso a ésta se efectuará de acuerdo a los privilegios asignados a los usuarios autorizados, conforme a la clasificación de la información establecida en el documento "Lineamientos para la clasificación de la información", y conforme a lo indicado en los ítems 9.3 y 9.4 del presente documento.

5.6 Cambio de Clave

El procedimiento para proporcionar en caso de cambios de clave, una nueva clave pública de la EC raíces o intermedias (no certificados de atributos), a los titulares y terceros aceptantes de los certificados que emite la EC.

En el caso que las claves empleadas para firmar un certificado válidamente emitido por la EC sean retenidas hasta la fecha de expiración de dichos certificados.

5.7 Recuperación frente al Compromiso y Desastre

5.7.1 Procedimiento de manejo de incidencias y compromisos

La EC BMCert establece los procedimientos a seguir en caso de ocurrir un evento o compromiso real o potencial de los mecanismos de comunicación, registro y de respuesta a incidentes, 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, deberán ser comunicados a través de canales pre-establecidos 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 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 fuere causado el fallo catastrófico) si la ER, que opera bajo la EC BMCert experimenta lo siguiente:

- Sospechoso o detectado compromiso en los sistemas de la ER;
- Penetración física o electrónica de los sistemas de la ER ; o
- Ataques de negación de servicio exitosos en los componentes de la ER

5.7.2 Adulteración de los recursos computacionales, software y/o datos

Cuando los recursos informáticos de la ER, 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 ER no se destruyeron, la operación de la ER se restablece restaurando el software de la copia de seguridad o reinstalando el software.
3. Si se destruyen las claves de firma ER, se vuelve a emitir la clave y el certificado de la ER y se restablece la operación lo más rápidamente posible.

El Oficial de Seguridad del MSO y el Oficial de Seguridad de BMCert son notificados tan pronto como sea posible.

5.7.3 Procedimientos en caso de compromiso de la clave privada de la entidad

En caso, la clave de la EC BMCert fuera comprometida de manera real o potencial, ésta deberá ser inmediatamente cancelada, notificándose el hecho en un lapso máximo de 24 horas a la AAC.

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

5.7.4 Capacidad de continuidad de negocio luego de un desastre

La EC BMCert dispone de procedimientos de recuperación para reconstituir la EC dentro de las 72 horas siguientes al fallo.

En el caso de un desastre por el cual la instalación que hospeda las aplicaciones y el servicio de la ER es físicamente dañada, el Oficial de Seguridad de BMCert y el Oficial de Seguridad del MSO serán notificados lo antes posible y ambos tomarán cualquier acción que consideren apropiada (ej. decir, determinar si y cuándo es posible restablecer el servicio de la ER), en este caso se podrá habilitar la EC BMCert Off-line.

En los casos en que las operaciones de la ER no se vean afectadas por tal evento (es decir, si existe una facilidad operacional alternativa que ofrezca los mismos controles de seguridad que la facilidad primaria y que está disponible), el Oficial de Seguridad de BMCert evaluará el estado del servicio de la ER para determinar qué capacidades, si las hubiere, no estarán disponibles hasta que las operaciones se restablezcan en la instalación primaria y hagan una determinación de cuánto tiempo las operaciones probablemente tendrán que permanecer en el sitio de contingencia. El Oficial de Seguridad de BMCert informará al Oficial de Seguridad del MSO del estado del servicio ER que estará operando desde el sitio alternativo. Corresponderá al Oficial de Seguridad del MSO determinar si modifica o no temporalmente el nivel de aseguramiento en el que opera la EC o toma otras acciones apropiadas.

Independientemente del impacto en las operaciones de la ER, los suscriptores serán informados a través

de algún método de notificación indicado (correos electrónicos, mensajes SMS al celular indicado o notificaciones electrónicas) de la determinación del Oficial de Seguridad del MSO y Oficial de Seguridad de BMCert.

5.8 Finalización de la EC o ER

En casos que la EC BMCert comunique a la ER la finalización de sus actividades, ésta última adoptará las medidas posibles para minimazar el impacto que pueda causar en los mienbros de la comunidad de usuarios a la que se alude en la sub seccion 1.3 del presente codumento.

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

6.0 CONTROLES DE SEGURIDAD TÉCNICA

La información contenida en esta sección es relativa a los controles técnicos de seguridad implementados por la EC BMCert en apoyo de su premisa en la infraestructura ER (por ejemplo, la aplicación ER).

6.1 Generación e instalación del par de claves

6.1.1 Generación del pares de claves

El par de claves de firma para los suscriptores de la EC que realizan roles de confianza (por ejemplo, EC BMCert y Business Partner ER) se genera utilizando un módulo de hardware criptográfico que se valida conforme a la norma FIPS 140 de nivel de seguridad 2 (o superior). El par de claves del Suscriptor se genera en medios criptográficos que cumplan con la certificación FIPS 140-2 nivel 2 ó CommonCriteria EAL4+ de una manera segura.

El par de claves de firma para suscriptores de nivel de Seguridad Media se genera utilizando un módulo criptográfico de software o hardware que se valida conforme a la norma FIPS 140 de nivel de seguridad 1 o superior. El par de claves del Suscriptor se genera en medios criptrograficos que cumplan con la certificación FIPS 140-2 nivel 2 ó CommonCriteria EAL4+ de una manera segura.

Todos los módulos criptográficos mencionados anteriormente funcionan de tal manera que las claves criptográficas asimétricas privada nunca se emiten en texto en claro (sin cifrar).

6.1.2 Entrega al suscriptor de la clave privada

Se generarán claves del certificado de firmas privadas y permanecerán dentro del límite criptográfico del módulo criptográfico del propietario de la clave.

La aplicación de la EC entregará las claves privadas que genera al suscriptor en una transacción en línea de acuerdo con RFC2510 (es decir, PKIX-CMP) o mediante una forma igualmente segura según lo especificado por la política local y aprobada por el Oficial de Seguridad del MSO y BMCert .

La entrega de un módulo con clave a su propietario será realizada por personal de confianza en las

instalaciones de la ER, esto se llevará a cabo en un ambiente de querantice la confidencialidad en la entrega de la clave privada.

6.1.3 Entrega de la clave pública para el emisor de un certificado

Las claves públicas se entregarán a la EC electrónicamente en una solicitud de certificado firmado. La solicitud de certificado se transmitirá a la EC utilizando su canal seguro, una sesión PKIX-CMP autenticada o mediante una forma igualmente segura según lo especificado por el presente documento.

6.1.4 Entrega de la clave pública de la EC al tercero que confía

La clave pública de la EC se entrega a los suscriptores utilizando uno de los métodos siguientes:

- El certificado de la EC se entrega al suscriptor que ejecuta un software de cliente de Entrust a través de una sesión segura de PKIX-CMP autenticada. El envío de datos de activación se realiza una sola vez para esta sesión por la ER al Suscriptor y sirve como autenticación de la clave de la EC.
- El certificado de la EC se entrega al Suscriptor utilizando una aplicación de distribución de software aprobada por la EC BMCert (por ejemplo, a través de las aplicaciones de la ER)
- El certificado de la EC puede ser descargado por el suscriptor de los servidores LDAP y HTTP recibidos por MSO-Entrust. http://www.bmtech.pe/root

Para las Partes de Confianza que no son suscriptores, la clave pública de la EC se entrega a los suscriptores utilizando uno de los métodos siguientes:

- El certificado de la EC puede ser descargado por el suscriptor de los servidores LDAP y HTTP publicados por MSO (Entrust).

La autenticidad del certificado puede ser verificada en contacto con el Oficial de Seguridad de la EC BMCert para confirmar la huella digital del certificado.

Todas las entidades emisoras subordinadas que hacen valer la política de la EC están subordinadas y obtienen su certificado EC de la entidad emisora raíz, la cual está autorizada para emitir certificados de la EC.

6.1.5 Tamaños de las claves

Todos los certificados emitidos por la EC son firmados digitalmente por la autoridad competente mediante el algoritmo de hash seguro 256 (SHA-256) algoritmo de hash.

Todos los certificados emitidos por el la EC BMCert contienen una clave pública RSA de 2048 bits.

6.1.6 Generación de parámetros de las claves públicas y verificación de la calidad

La EC BMCert debe generar sus pares de claves de acuerdo con RFC 3280 y PKCS#1.

6.1.7 Propósitos del uso de las claves (conforme a lo establecido en el campo de uso de x.509 v3)

Las claves son certificadas para su uso en la firma, no repudio. Todos los certificados emitidos por la

EC utilizan la extensión *keyUsage* para gobernar el uso de una clave específica.

Los certificados de suscriptor que se utilicen para las firmas digitales establecen tanto el bit *digitalSignature* y el bit de *nonRepudiation* (no repudio).

Los certificados de suscriptor que contienen las claves públicas RSA que se utilizarán para el transporte de claves definen el bit *keyEncipherment*.

Certificados de la EC tienen los bits *keyCertSign* y *cRLSign* establecidos.

Los bits *dataEncipherment*, *encipherOnly*, y *decipherOnly* no se hacen valer en los certificados emitidos bajo esta política.

6.2 Controles de ingeniería para protección de la clave privada y módulo criptográfico

6.2.1 Estándares y controles para el módulo criptográfico

La norma pertinente para los módulos criptográficos es la versión más reciente de la serie FIPS 140-2 nivel2 y Common Criteria EAL4+ (*Requisitos de Seguridad para Módulos Criptográficos)*.

6.2.2 Control Multi-Persona de la Clave Privada

No estipulado.

6.2.3 Depósito de clave privada

La EC BMCert no admite el depósito, almacenamiento o copia de claves privadas,utilizadas para la firma y autenticación digital de los usuarios finales, ni de los módulos 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 de los PSCs

No se realiza copia de seguridad de la clave privada de la EC BMCert y éstas no pueden ser utilizadas fuera del HSM.

6.2.5 Archivo de la clave privada

Las claves privadas de suscriptores o titulares no serán archivadas.

6.2.6 Transferencia de la clave privada de o hacia un módulo criptográfico

La EC generará claves privadas en nombre de suscriptores de entidades finales dentro de su propio kernel criptográfico de software. La clave privada se transportará de forma segura al suscriptor utilizando un protocolo seguro, como las sesiones SSL o PKI-CMP.

6.2.7 Almacenamiento de la clave privada en un módulo criptográfico

No existe ninguna estipulación más allá de lo especificado en FIPS 140-2.

6.2.8 Método de activación de la clave privada

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 de desactivación de la clave privada

El suscriptor o titular debe desactivar su clave privada mediante el mecanismo especificado por el fabricante del componente (del medio portador) que almacena dicha clave.

6.2.10 Método de destrucción de la clave privada

Las claves privadas ubicadas en el módulo criptográfico de hardware se destruyen reiniciando el módulo criptográfico utilizando una utilidad suministrada por el proveedor. La clave privada también puede destruirse destruyendo físicamente el token.

Si el requierente de la destrucción de la clave privada es el suscriptor o titular, primero deberá realizarse el procedimiento de cancelación del certificado y luego debe eliminar su clave privada.

6.2.11 Clasificación del módulo criptográfico

Los módulos criptográficos usados por la EC BMCert cumplen los requerimientos de FIPS 140-2 nivel de seguridad 3 y Common Criteria EAL4+

Más detalles de los módulos criptográficos son indicados anteriormente en la Sección 6.2.1.

6.3 Otros aspectos de la gestión del par de claves

6.3.1 Archivo de la clave pública

La EC mantiene un archivo de todos los certificados de clave pública que emite.

6.3.2 Períodos operacionales del certificado y periodo de uso de las claves

A continuación, los periodos operacionales de los certificados:

Ítem	Tipo del Certificado	Tiempo	Tamaño de clave
Clase I	Autenticación y/o firma digital para persona jurídica	1, 2 o 3 años	2048
Clase II	Persona Jurídica (Agente Automatizado)	1, 2 o 3 años	2048
Clase III	Autenticación y/o firma digital para persona natural	1, 2 o 3 años	2048
Clase IV	Autenticación y/o firma digital para persona natural con negocio	1, 2 o 3 años	2048
Clase V	Persona Natural Profesional	1, 2 o 3 años	2048

Otros tipos de certificados pueden ser generados únicamente en la EC off-line, previa especificación a la AAC.

6.4 Datos de activación

6.4.1 Generación e instalación de datos de activación

Los datos de activación del acceso a la clave privada debe ser realizada por el suscriptor como mínimo mediante el uso de contraseña (es decir, no biométrica o un PIN), los utilizados por los suscriptores están obligados a ajustarse a una política definida en acuerdo con la ER.

6.4.2 Protección de los datos de activación

Las ERs deben tener acceso a las funciones de la EC mediante un token criptografico (hardware) asignados a ellos que contienen sus claves criptográficas. El uso del token de hardware requiere la introducción de una contraseña única conocida únicamente por el propietario del token.

La protección del token de hardware es responsabilidad de la persona que llena el rol de confianza.

El uso del token hardware/software requiere la introducción de una contraseña única conocida únicamente por el propietario del token. La protección del token es responsabilidad del suscriptor.

6.4.3 Otros aspectos de los datos de activación

Las ERs deben tener acceso a las funciones de la EC mediante un token criptografico (hardware) asignados a ellos que contienen sus claves criptográficas. El uso del token de hardware requiere la introducción de una contraseña única conocida únicamente por el propietario del token. Después de 3 intentos fallidos consecutivos de entrada de contraseña, el token se bloquea permanentemente y no se puede recuperar para su reutilización sin que todo el material de clave sea puesto a cero (el token debe reinicializarse). El suscriptor deberá apersonarse a una oficina de la ER para obtener un nuevo token y recuperar su cuenta de suscriptor del rol de confianza de la EC.

Los datos de activación de los módulos criptográficos para los que se transfiere el control (como cuando una persona que actúa en un rol de confianza salen de la organización) se reinicializará y se devolverá al inventario o se cargará con las credenciales de una nueva persona para servir en su papel de confianza asignado.

También el suscriptor puede determinar que otros aspectos son necesarios a considerar, para mantener una mejor protección de la clave privada de su certificado, por ejemplo, puede requerirse el cambio de PINs y contraseñas cada 30 días.

6.5 Controles de seguridad computacional

6.5.1 Requisitos técnicos específicos para seguridad computacional

La EC BMCert hosteda en los Servicios Ofrecidos por ENTRUST, 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 ER; 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 Evaluación de la seguridad computacional

No aplica.

6.6 Controles técnicos del ciclo de vida

Estos controles aplican a los componentes de hardware y software que conforman toda la plataforma tecnológica de la EC BMCert usados para proporcionar servicios de certificación digital.

La eficacia y la idoneidad de las prácticas descritas en esta CPS son revisadas cuando sean decididas por el Oficial de Seguridad de BMCert.

También se lleva a cabo una evaluación de riesgo y amenazas para determinar si se deben incrementar las longitudes de clave o modificar los procedimientos operativos para mantener el nivel requerido de seguridad del sistema.

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 ER 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 notifica al Oficial de Seguridad del MSO y 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 ER.

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 ER. Las protecciones de seguridad física restringen la posibilidad de que el software malicioso se inserte en el servidor que aloja la aplicación de la ER. 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 ER.

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 ER. 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 la 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 ER 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 notifica al Oficial de Seguridad del MSO y coordina la respuesta del incidente con el personal apropiado.

6.6.3 Evaluación 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 ER, 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 ER. 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 ER.

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 ER es necesario para el correcto funcionamiento de esta.

6.8 Sello de tiempo

Todas las transacciones registradas producidas por los servicios de la ER son automáticamente selladas

por el servicio de PKI (MSO de Entrust) como parte de las operaciones normales. Como se describió anteriormente en la Sección 5.5.4, la exactitud de la marca de tiempo se mantiene mediante el uso de un servidor de tiempo de red (NTP Server) utilizando un proceso de consistencia establecida entre datos de una fuente a un almacenamiento de datos objetivo y viceversa y la armonización continua de los datos a cada hora.

7.0 CERTIFICADO Y PERFILES DE LCR (CRL)

7.1 Perfil del Certificado

7.1.1 Número(s) de Versión(es)

Soporta y emplea el estándar x.509 v3.

El certificado emitido por la EC contempla el contenido y campos descriptos en el ítem 3.1.1 del presente documento, además de los seguintes:

- Numero de serie, que será un código uno con respecto al DN del emisor.
- Algoritmo de firma
- El DN del Emisor
- Inicio Validez del certificado baseado en la RFC3280
- Fin Validez del certificado baseado en la RFC3280
- Nombre distinguido del Suscriptor
- Clave Publica de acuerdo a la RFC 3280
- Firma de acuerdo a la RFC 3280
- Uso Autorizado del Certificado Digital

7.1.2 Extensiones del certificado

El certificado soporta todas las extensiones de certificado x.509 v3.

7.1.3 Identificadores de Objeto de algoritmo

Los Certificados emitidos deben usar por lo menos uno del siguiente algoritmo:

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

7.1.4 Forma de Nombres

El formato de nombres está de acuerdo al formato distinguidos x.501 asi como especifica en la sección 3.1.1 dicho documento.

7.1.5 Restricciones de Nombre

Las restricciones de nombre se establece en la RFC 3280, únicos y no ambiguos (DN x.500).

7.1.6 Identificador de Objeto de la Política de Certificados

Certificados de la EC BMCert y certificados de Suscriptor emitidos de conformidad con el presente documento, es válido uno o más de los siguientes OIDs en la extensión de políticas de certificado, según el caso tiene un identificador de objeto (OID), el cual es: 2.16.840.1.114027.200.3.10.39

7.1.7 Extensión de Restricciones de uso de la política

No aplica

7.1.8 Sintaxis y Semántica de los calificadores de la política

No aplica

7.1.9 Procesamiento de Semántica para la extensión de políticas de Certificados Críticos

No aplica

7.2 Perfil CRL

Parameter	BMCert Root CA	BMCert Issuing CAs
CA DNs	cn=BMCERT Root CA, ou=Certification Authorities, o=BMCERT, c=PE	cn=BMCERT Issuing CA, ou=Certification Authorities, o=BMCERT, c=PE
CA Type	Self-Signed Root CA	Subordinate CA
Online/Offline Mode	Online/Offline	Online
CA key pair algorithm	RSA-2048	RSA-2048
CA database encryption algorithm	AES-256	AES-256
Signing Certificate Hashing Algorithm	SHA-256	SHA-256
Hardware base database protection (i.e. database encryption key stored on the HSM)	Yes	Yes
Policy Certificate Lifetime is good for	30 days	30 days
CA Certificate Lifetime	December 2030 (NIST Recommendation for RSA-2048)	December 2027 (Root CA certificate lifetime – Subscriber certificate lifetime (36 months))
Private Key Usage Period	100%	100%
Administration Service (ASH) port	710	710
PKIX-CMP port	829	829

Parameter	BMCert Root CA	BMCert Issuing CAs
Secure Exchange Protocol (SEP) port	N/A	709
XAP enabled	No	Yes – 1443
Enabled for MS Application	Yes, compatibility with all Windows platforms	Yes, compatibility with all Windows platforms
CRL lifetime	1 year –BMCert Root CA	Published once every 6 hours, with next scheduled update periods specified every 72 hours
Issue combined CRL to LDAP	Yes	Yes

7.2.1 Numero de Versiones

CRL X.509 v2

Certificados X.509 v3

7.2.2 Extensiones de Entrada de CRL

En acuerdo con la RFC3280

7.3 Perfil OCSP

OCSP no es usado por la EC BMCert.

7.3.1 Numero de Versión

OCSP no es usado por la EC BMCert.

7.3.4 Extensiones OCSP.

OCSP no es usado por la EC BMCert.

8.0 AUDITORÍAS DE COMPATIBILIDAD Y OTRAS EVALUACIONES

La información contenida en esta sección es específica de la auditoría de cumplimiento y otras evaluaciones implementado por la EC BMCert soportando sus servicios de ER.

Dicho documento cubre la auditoría de cumplimiento específico implementado por MSO de los componentes del PKI alojados y operados por Entrust (por ejemplo, CA, Directorio, Hardware Security Module – HSM).

8.1 Frecuencia o circunstancias de Evaluación

El cumplimiento de las auditorías de los servicios de la ER se llevan 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 (por ejemplo, ER IOFE-SAC) del PKI 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, según lo permitido por el CP, 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 de Asesores

El Oficial de Seguridad de la EC BMCert tiene la responsabilidad de auditar los componentes de la ER 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 ER puede ser realizado 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 PKI, 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 auditor con la entidad auditada

La realización de la auditoría de cumplimiento de la ER es nombrado 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 (BMTECH PERU SAC).

8.4 Elementos 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 ER y todas las personas que realizan los Roles de Confianza con el PKI satisfacen todos los elementos de este CPS y la DPR.

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 ER.
e) Controles de seguridad técnicos.

8.5 Acciones a ser tomadas frente a resultados deficientes

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 de la Compliance Auditor y el Oficial de Seguridad del MSO, determinará qué punto del espectro está justificada. 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 llevaron 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 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 ó 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, Oficial de Seguridad del MSO y Compliance Auditor, el equipo de auditoría de cumplimiento realizará la re-auditoría del servicio de ER 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 y el Oficial de Seguridad del MSO van 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 presentadas 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 establecido en "sustituido". El Oficial de Seguridad de BMCert es responsable de informar sobre el estado de las acciones correctivas al Oficial de Seguridad del MSO y auditores diariamente.
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. El Oficial de Seguridad de BMCert es responsable de reportar el estado de la acción correctiva al Oficial de Seguridad del MSO y de los auditores diariamente.
4. Si se toma la acción 4 el Oficial de Seguridad de BMCert pedirá al Oficial de Seguridad del MSO para solicitar 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 por el Oficial de Seguridad del MSO 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 re-inscritos 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 re-emisión 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. El Oficial de Seguridad de BMCert es responsable de informar sobre el estado de las acciones correctivas y la migración de abonado al Oficial de Seguridad del MSO y las

cuentas sobre una base diaria. 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 cual de estas acciones basada en la severidad de las irregularidades a ser tomada.

8.6 Publicación de Resultados

El Auditor de Cumplimiento comunicará los resultados a todas las ER de las auditorías de cumplimiento de servicio al Oficial de Seguridad del MSO y 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 la PKI para no cumplir 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 ER y los servicios de la ER y los temas en los que la ER 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 y Oficial de Seguridad del MSO.

9.0 OTRAS MATERIAS DE NEGOCIO Y LEGALES

9.1 Tarifas

9.1.1. Tarifas para la 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 a certificados

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

9.1.3 Tarifas para información sobre revocación o estado

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

9.1.4. Tarifas para 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. Políticas 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 del negocio

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. Alcances 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 no contenida dentro del rubro de 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 protección de 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. Pricavidad 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 revelarsu 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 brinadado 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 protección de 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. Notificación y consentimiento para el uso de información

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 realizada con motivo de 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 para 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 de la 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. Representaciones y garantías de la 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 la ER

No aplica.

9.6.3. Representaciones y garantías de los suscriptores

Las obligaciones de los sucriptores 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 IOFE S.A.C a la cual está vinculada o de cualquier otra ER que se encuentre 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 IOFE S.A.C a la cual está vinculada o de cualquier otra ER que se encuentre acreditada ante la AAC 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 IOFE S.A.C a la cual está vinculada o de cualquier otra ER que se encuentre acreditada ante la AAC. en dicho acuerdo estarán contenidas las consecuencias de eventuales incumplimientos. El acuerdo contemplará las obligaciones establecidas porla 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 IOFE S.A.C a la cual está vinculada o de cualquier otra ER que se encuentre acreditada ante la AAC 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 garantias de los terceros que confían

Las partes que confian 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 garantias 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. Exención 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 a la 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. Término y terminación

9.10.1. Término

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 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. Notificaciones y comunicaciones individuales 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. Enmendaduras

9.12.1 Procedimiento para enmendaduras

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

9.12.2 Mecanismos y periodo 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 Ecde BMCert, asi como acuerdos de certificación cruzada, siempre que dichos cambios puedan afectarles.

La ER IOFE S.A.C a la cual está vinculada o de cualquier otra ER que se encuentre acreditada ante la AAC notificará estos 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 debe ser cambiado el IOD

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

9.13. Provisiones sobre 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. Conformidad con 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. Cláusulas misceláneas

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 íntegro

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. Subogración

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 (tarifas de abogados y cláusulas 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 cláusulas

No aplica.

10.0 BIBLIOGRAFÍA

- Ley N° 27269, de Firmas y Certificados Digitales
- Ley N° 29733, de Protección de Datos Personales.
- Reglamento de la Ley de Firmas y Certificados Digitales aprobado mediante el Decreto Supremo Nº 052-2008-PCM, y su modificatoria, el Decreto Supremo N° 070-2011-PCM.
- Reglamento General de Acreditación de Prestadores de Servicios de Certificación
- Digital (PSC), establecido porla Autoridad Administrativa Competente (AAC).
- Reglamento específico de Acreditación para Entidades de Certificación Digital y Entidades Conexas (guía), expedido por la AAC.
- ANEXO 1: MARCO DE LA POLÍTICA DE EMISIÓN DE CERTIFICADOS DIGITALES, expedido por la AAC.
- Decreto Supremo Nº 070-2011, que modifica el Reglamento de la Ley Nº 27269, Ley de firmas y certificados digitales y establece normas aplicables al procedimiento registral en virtud del Decreto Legislativo Nº 681 y ampliatorias.