DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN

VERSIÓN: V2.6

PUBLICO

OFICIAL

PARA: LLAMA.PE

HISTORIAL DE VERSIONES

VERSIÓN	DESCRIPCIÓN	REALIZADO POR	FECHA
V2.6	Actualización en el punto 28.6	LOUIE ALBERTO DIAZ MARTICORENA	2023-09-11
V2.5	Precisión de los tipos de certificados digitales de facturación electrónica, profesional y OSE en el punto 7.1	JORGE ENRIQUE MIGUEL ZELAYARÁN SANCHEZ	2023-06-26
V2.4	Al utilizar un nuevo formato documento, se detallan todas los cambios en las versiones anteriores hasta la versión actual (v2.4): - 1.1: Se agrega a Persona Natural como un nuevo tipo de certificado. Se detallan los controles de seguridad física. Se modifican los roles de confianza. - 1.2: Se modifica la estructura del documento. Se especifican los enlaces para acceder al Repositorio. - 1.3: Se modifica conceptos y actualización para brindar el servicio a nuevas ER. - 1.4: Se modificaron los criterios para la interoperabilidad a fin de soportar otras Entidades de Registro. - 1.5: Se actualizó el término suspensión. Se actualizaron los links de los repositorios en www.llama.pe. - 1.6: Se agrega información relacionada a la Autoridad de Sellado de Tiempo. - 1.7: Se actualiza el concepto de remisión y se hacen cambios en los datos del responsable de la EC. - 1.8: Se agrega un inciso concerniente a las ER anexas a la Entidad de Certificación de Llama.pe. - 1.9: Actualización de formatos. - 2.0: Actualización del punto 19.1. - 2.1: Actualización del punto 28.6 y 28.10. - 2.2: Se agregó el apartado 32 Resolución de disputas, precisión en el apartado 31.3. - 2.3: Se agrega un punto que habla sobre el acceso mediante IP de las ER anexas en el inciso 31.6.3. - 2.4 (versión actual): Precisión en el punto 31.6.3 respecto a la verificación de antecedentes de los Operadores de Registro.	JORGE ENRIQUE MIGUEL ZELAYARÁN SANCHEZ	2023-01-03
V1.0	Se agrega un punto que habla sobre el acceso mediante IP de las ER anexas en el inciso 31.6.3	LOUIE ALBERTO DIAZ MARTICORENA	2022-12-27

Tabla de contenido

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN

1 INTRODUCCIÓN

LLAMA.PE S.A., que en adelante llamaremos “LLAMA.PE”, es una empresa peruana fundada en el año 2013 con el compromiso de proveer seguridad digital a personas y organizaciones de todo tipo en el uso de aplicaciones web.

Actualmente las soluciones que LLAMA.PE ofrece, se extienden a soluciones PKI escalables basadas en la nube para instituciones financieras, gobiernos, organizaciones de todo tipo y empresas que tienen que realizar comercio, las comunicaciones, entrega de contenido e interacciones con la comunidad digital de forma segura.

Entre los tipos de certificados digitales que provee son: Certificado digital para Factura Electrónica según lo solicitado por SUNAT en el Perú para firmar archivos XML, Certificados SSL para páginas web, correo electrónico, PDF, autenticación, firma de código, etc.

En el año 2017, LLAMA.PE logró acreditarse como Entidad de Certificación y como Entidad de Registro para proveer los servicios de emisión, re-emisión y revocación de certificados digitales.

En calidad de Entidad de Registro, LLAMA.PE brinda los servicios de registro o verificación de sus clientes, tanto en el caso de personas jurídicas como naturales.

En calidad de Entidad de Certificación, LLAMA.PE presta servicios de emisión, revocación y re-emisión de certificados digitales siguiendo la regulación establecida por el marco de la IOFE.

Esta DPC establece las prácticas que lleva a cabo "LLAMA.PE". para emitir, gestionar, revocar y

renovar certificados digitales, siguiendo el estándar RFC 3647 “Internet X.509 Public Key Infrastructure

Certificate Policy and Certification Practices Framework”.

2 OBJETIVO

Este documento tiene como objeto la descripción de las operaciones y prácticas que utiliza LLAMA.PE para la administración de sus servicios como Entidad de Certificación Digital – EC, en el marco del cumplimiento de los requerimientos de la “Guía de Acreditación de Entidades de Certificación Digital (EC)” establecida por el INDECOPI. Asimismo, el presente documento se encuentra en concordancia con la Política de Seguridad de LLAMA.PE, la cual garantiza que la seguridad de la información que es tratada durante todo el proceso de certificación digital.

3 OBJETO DE LA ACREDITACIÓN

El alcance de la acreditación cubre la infraestructura y procesos de los servicios de certificación digital de LLAMA.PE.

LLAMA.PE representa todos los aspectos de responsabilidad y mediación entre las personas jurídicas y naturales del Estado Peruano.

4 DEFINICIONES Y ABREVIACIONES

4.1 ABREVIACIONES

AAC: Autoridad Administrativa Competente

DN: (Distinctive Name) Nombre Distintivo

EC: Entidad de Certificación

ER: Entidad de Registro

CPS: (Certification Practice Statement) Declaración de Prácticas de Certificación

CRL: Lista de Certificados Revocados

IOFE: Infraestructura Oficial de Firma Electrónica

PC: Política de Certificación

RUC: Registro Único de Contribuyentes

SHA: Secure Hash Algorithm (Algoritmo de seguridad HASH)

CA: Cetification Authority (Autoridad de Certificación)

DSCF: Dispositivo seguro de creación de firma

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

IEC: International Electrotechnical Commission

ISO: International Organization for Standardization

PKCS: Public-Key Cryptography Standards.

PKI: Infraestructura de llave pública

PSC: Prestador de Servicios de Certificación

RA: Autoridad de Registro

RFC: Request For Comments

RSA: Rivest, Shamir y Adleman.

SSL: Secure Sockets Layer

TSA: Time Stamping Authority

TSU: Time Stamping Unit

4.2 DEFINICIONES

- Entidad de Certificación – EC: Entidad que presta servicios de emisión, revocación, re-emisión de certificados digitales en el marco de la regulación establecida por la IOFE.
- Entidad de Registro – ER: Entidad que realiza los procesos de verificación de identidad de los solicitantes de los servicios de certificación digital y que se encarga de custodiar esta misma información.
- Política de Certificación: Conjunto de reglas que indican el marco de aplicabilidad de los servicios para una comunidad de usuarios definida.
- Autoridad de Sellado de Tiempo – TSA: Conjunto de datos que representa el resumen de un documento sellado añadido a un registro del tiempo en el que el sello fue emitido. Este resumen es una característica única del documento, de modo que si el documento es modificado este sello pierde validez.
- Unidad de Sellado de Tiempo – TSU: Componentes de hardware y software que son administrados como una unidad para proveer sellos de tiempo desde una fuente de tiempo.

- Titular: Entidad que requiere los servicios provistos por la EC, y que está de acuerdo con los términos y condiciones de los servicios conforme a lo declarado en el presente documento.
- Tercero que confía: Persona que recibe un documento, log, o notificación firmado digitalmente, y que confía en la validez de las transacciones realizadas.
- Algoritmo: es un conjunto prescrito de instrucciones o reglas bien definidas, ordenadas y finitas que permite realizar una actividad mediante pasos sucesivos que no generen dudas a quien deba realizar dicha actividad. Dados un estado inicial y siguiendo los pasos sucesivos se llega a un estado final y se obtiene una solución.
- Certificado digital: mensaje de datos electrónico firmado por la entidad de certificación digital, el cual identifica tanto a la entidad de certificación que lo expide, como al suscriptor y contiene la llave pública de este último.
- Cliente: En los servicios de certificación digital, el término cliente identifica a la persona natural o jurídica con la cual la EC establece una relación comercial.
- Datos de Creación de Firma (Llave privada o clave privada): son valores numéricos únicos que, utilizados conjuntamente con un procedimiento matemático conocido, sirven para generar la firma digital de un mensaje de datos.
- Declaración de Prácticas de Certificación: Es el documento en el que consta de manera detallada los procedimientos que aplica la EC para la prestación de sus servicios. Una declaración de las prácticas que una EC emplea para emitir, gestionar, revocar y renovar certificados sin y con cambio de claves.
- Declaración de Prácticas del Servicio de Valor Añadido para la TSA: Conjunto de declaraciones acerca de políticas y prácticas que dirigen las actividades y procesos de la TSA y que son publicadas para conocimiento de suscriptores y terceros que confían.
- Política de Sellado de Tiempo: Conjunto de directivas que dirigen la aplicabilidad y requisitos en la administración de un servicio de sello de tiempo para una determinada comunidad de usuarios y un determinado alcance.
- Dispositivo seguro de creación de firma: Elemento software o hardware empleado por el suscriptor para la generación de firmas digitales, de manera que se realicen las operaciones criptográficas dentro del dispositivo y se garantice su control únicamente por el suscriptor.
- FIPS: Federal Information Processing Standards(FIPS, en español Estándares Federales de Procesamiento de la Información) son estándares anunciados públicamente desarrollados por el gobierno de los Estados Unidos para la utilización por parte de todas las agencias del gobierno no militares y por los contratistas del gobierno. Muchos estándares FIPS son versiones modificadas de los estándares usados en las comunidades más amplias (ANSI, IEEE, ISO, etc.)
- Firma Digital: Se entenderá como un valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático reconocido, vinculado a la clave del iniciador y al texto del mensaje permite determinar que este valor se ha obtenido exclusivamente con la clave del iniciador y que el mensaje inicial no ha sido modificado después de efectuada la transformación.
- Función Hash o Hash: es una operación que se realiza sobre un conjunto de datos de cualquier tamaño, de forma que el resultado obtenido es otro conjunto de datos de tamaño fijo, independientemente del tamaño original, y que tiene la propiedad de estar asociado unívocamente a los datos iniciales.
- Lista de Certificados Digitales Revocados: es aquella relación que debe incluir todos los certificados revocados por la entidad de certificación digital.
- Log: Servicio de registro de eventos del sistema de información, dejando la información anterior y la actual, identifica quién y cuándo se realizó el evento.
- PKI: Infraestructura de llave pública (Public key infraestructure): es el conjunto de hardware, software, políticas, procedimientos y elementos tecnológicos que, mediante la utilización de un par de claves criptográficas, una privada que sólo posee el suscriptor del servicio y una pública, que se incluye en el certificado digital, logran: Identificar al emisor de un mensaje de datos electrónico, impedir que terceras personas puedan observar los mensajes que se envían a través de medios electrónicos, impedir que un tercero pueda alterar la información que es enviada a través de medios electrónicos y evitar que el suscriptor del servicio de certificación digital que envió un mensaje electrónico pueda después negar dicho envío (no repudio).
- PKCS: Public-Key Cryptography Standards. Estándares de criptografía de llave pública concebidos y publicados por los laboratorios de RSA. Anexo G
- Políticas de Certificado: Es el conjunto de reglas que indica los requisitos de un certificado en una comunidad y/o clase en particular, en el marco de los requisitos legales, reglamentarios, y con requisitos de seguridad comunes.
- RFC: Request for Comments son una serie de publicaciones del Internet Engineering Task Force (IETF) que describen diversos aspectos del funcionamiento de Internet y otras redes de computadoras, como protocolos, procedimientos, etc.
- RSA: Rivest, Shamir y Adleman. Es un sistema criptográfico de llave pública desarrollado en 1977. Es el primer y más utilizado algoritmo de este tipo y es válido tanto para cifrar como para firmar digitalmente.
- Servicio de certificación digital: Conjunto de actividades de certificación que ofrece la EC para certificar el origen e integridad de mensajes de datos, basados en las firmas digitales o electrónicas, estampado de tiempo, así como en la aplicabilidad de estándares técnicos admitidos y vigentes en infraestructura de llave pública.
- Solicitante: persona natural o jurídica que con el propósito de obtener servicios de certificación digital de una EC, demuestra el cumplimiento de los requisitos establecidos en la DPC y PC de éstas, para acceder al servicio de certificación digital.

- SSL: Secure Sockets Layer: capa de conexión segura. Protocolo criptográfico que proporciona comunicaciones seguras por una red, comúnmente Internet.
- Suscriptor: persona natural o jurídica a cuyo nombre se expide un certificado digital.
- Token: Dispositivo hardware criptográfico suministrado por una EC, el cual contiene el certificado digital y la llave privada del suscriptor.

4.3 PKI PARTICIPANTES

4.3.1 ENTIDAD DE CERTIFICACIÓN LLAMA.PE (EC LLAMA.PE)

LLAMA.PE, en su papel de Entidad de Certificación, es la persona jurídica privada que presta indistintamente servicios de producción, emisión, gestión, cancelación u otros servicios inherentes a la certificación digital.

Llama.pe, como Entidad de Certificación, le corresponderá la realización de todos los trámites y procedimientos administrativos necesarios ante la AAC a fin de poder ingresar a la IOFE.

Asimismo, dentro de sus funciones se encuentran las siguientes:

• Garantizar la seguridad, disponibilidad y calidad de las operaciones de gestión de los certificados digitales de los usuarios finales.
• Garantizar la seguridad de las claves de la EC Raíz y las EC Subordinadas durante todo su ciclo de vida.
• Garantizar la disponibilidad y accesibilidad de los servicios de consulta de estado de revocación de los certificados digitales.
• Garantizar la protección de los datos personales de los usuarios finales.
• Garantizar la continuidad del servicio a los titulares durante todo el tiempo en que se hayan contratado los servicios de certificación digital.

4.3.2 ENTIDAD DE REGISTRO LLAMA.PE (ER LLAMA.PE)

Llama.pe, brinda también los servicios de Entidad de Registro, la cual es la encargada de certificar la validez de la información suministrada por el solicitante de un certificado digital, mediante la verificación de su identidad y su registro.

4.3.3 AUTORIDAD DE SELLADO DE TIEMPO (TSA LLAMA.PE)

Llama.pe brinda también los servicios de Autoridad de Sellado de Tiempo, la cual se encarga de emitir sellos de tiempo. Un sello de tiempo es un conjunto de datos que representa el resumen de un documento sellado añadido a un registro del tiempo en el que el sello fue emitido. Este resumen es una característica única del documento, de modo que si el documento es modificado este sello pierde validez.

Las particularidades sobre el uso, perfiles y especificaciones de la TSA, se describen en la respectiva Política de Sellado de Tiempo de Llama.pe.

4.3.4 TITULAR

Titular es la persona natural o jurídica a cuyo nombre se expide un certificado digital y por tanto actúa como responsable del mismo confiando en él, con conocimiento y plena aceptación de los derechos y deberes establecidos y publicados en la CPS.

La figura de Titular será diferente dependiendo de los distintos certificados emitidos por LLAMA.PE, conforme a lo establecido en la Política de Certificación.

4.3.5 SUSCRIPTOR

Conforme a la IOFE, el Suscriptor es la persona natural responsable del 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 del 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 corresponderá a la persona jurídica. La atribución de responsabilidad del suscriptor, para tales efectos, corresponde a la misma persona jurídica.

4.3.6 SOLICITANTE

Se entenderá por Solicitante, la persona natural o jurídica que solicita un certificado emitido bajo el documento CPS.En el caso de los certificados de persona natural puede coincidir con la figura del Titular.

4.3.7 TERCERO QUE CONFÍA

Tercero que confía son todas aquellas personas naturales o jurídicas que deciden aceptar y confiar en los certificados digitales emitidos por la Entidad de Certificación de Llama.pe, a un titular. El Tercero que confía, a su vez puede ser o no titular.

4.3.8 ENTIDAD A LA CUAL SE ENCUENTRA VINCULADO EL TITULAR

En su caso, la persona jurídica u organización a la que el Titular se encuentra estrechamente relacionado mediante la vinculación acreditada en el certificado.

5 SERVICIOS DE CERTIFICACIÓN DIGITAL

LLAMA.PE brinda los servicios de emisión, re-emisión, revocación de certificados digitales.

Los certificados y las prácticas relacionadas a la gestión de su ciclo de vida son descritas en la Declaración de Prácticas y las Políticas de Certificación de Llama.pe, publicadas en:

https://llama.pe/repository

6 RESPONSABILIDADES

Las responsabilidades contractuales, garantías financieras y coberturas de seguros son brindadas por la Entidad de Certificación LLAMA.PE.

LLAMA.PE representa todos los aspectos de ejecución de obligaciones contractuales, responsabilidad y mediación entre las personas jurídicas y naturales del Estado Peruano y la Entidad de Certificación.

Asimismo, LLAMA.PE brinda los servicios de registro o verificación conforme a las Guías de Acreditación del INDECOPI, para realizar la verificación de identidad de los solicitantes de los certificados digitales.

Las peticiones, quejas o reclamos para la atención de suscriptores y terceros debido a consultas relacionadas con el servicio que dispone la EC, son recibidas directamente por LLAMA.PE mediante la línea telefónica o correo electrónico. Asimismo, pueden acercarse hacia la

oficina de ER de LLAMA.PE, indicando que presenta una queja, reclamo o petición. Los datos de Contacto se encuentran en la sección 8 de la CPS.

7 USO DEL CERTIFICADO

7.1 TIPOS DE CERTIFICADO

LLAMA.PE emite los siguientes tipos de certificados:

- Certificado de Persona Natural: Es el tipo de certificado que permite a una persona natural acreditarse y firmar digitalmente como tal, asumiendo la responsabilidad de suscriptor y titular de dicho certificado. Dentro de este tipo de certificados, se encuentran los certificados de profesional como persona natural.
- Certificado de Persona Jurídica: Es el tipo de certificado que identifica al firmante como Representante legal o Apoderado de una Organización o Entidad. Dentro de este tipo de certificados, se encuentran los certificados de profesional vinculado a una empresa y de atributos (identifica al firmante como colaborador, funcionario, entre otros).
- Certificado de Agente Automatizado: Es el tipo de certificado que identifica a un dispositivo informático perteneciente a una persona jurídica que realiza las operaciones de firma y descifrado de forma automática, y cuyas acciones se encuentran bajo la responsabilidad del suscriptor del certificado. Dentro de este tipo de certificados, se encuentran los de Operador de Servicios Electrónicos (OSE) y de facturación electrónica.
- Certificados para Sellado de Tiempo: La TSA emite certificados a una Unidades de Sellado de Tiempo - TSU.

Dichas TSU son las que proveen sellos de tiempo desde una fuente de tiempo confiable al recibir una solicitud estandarizada que siga las especificaciones del RFC 3161.

LLAMA.PE cuenta con una Política de Sellado de Tiempo que detalla este servicio.

7.2 USOS ADECUADOS DEL CERTIFICADO

Los Certificados emitidos bajo esta CPS pueden ser utilizados con los siguientes propósitos:

- Identificación del Titular: El Titular del Certificado puede autenticar, frente a otra parte, su identidad, demostrando la asociación de su clave privada con la respectiva clave pública, contenida en el Certificado.
- Integridad del documento firmado: La utilización del Certificado garantiza que el documento firmado es íntegro, es decir, garantiza que el documento no fue alterado o modificado después de firmado por el Titular. Se certifica que el mensaje recibido por el Receptor o Destino que confía es el mismo que fue emitido por el Titular.
- No repudio de origen: Con el uso de este Certificado también se garantiza que la persona que firma el documento no puede repudiarlo, es decir, el Titular que ha firmado no puede negar la autoría o la integridad del mismo.

7.3 USOS PROHIBIDOS DEL CERTIFICADO

Los Certificados emitidos bajo esta CPS no pueden ser utilizados para las siguientes circunstancias:

- Cuando contravengan la Ley de Firmas y Certificados Digitales – Ley 27269, las Guías de Acreditación del INDECOPI o sus anexos.

8 PERSONA DE CONTACTO

Datos de la Entidad de Certificación y Entidad de Registro:

Nombre: LLAMA.PE S.A.

Dirección: Ca. Libertad 176 Oficina 202 - Soho, Miraflores

Domicilio: Lima

Teléfono: 01 3012200

Correo electrónico: hola@llama.pe

Página Web: https://llama.pe/

9 RESPONSABILIDADES DE LOS TITULARES Y SUSCRIPTORES

Los usuarios y solicitantes de los certificados digitales provistos por LLAMA.PE son responsables de revisar la presente CPS y Políticas de LLAMA.PE, a fin de ser enterados de las características de la plataforma de servicios, infraestructura y procedimientos empleados en la gestión del ciclo de vida de los certificados digitales, Raíz, Intermedios y de usuario final, así como las obligaciones de cada parte.

10 ORGANIZACIÓN QUE ADMINISTRA LOS DOCUMENTOS DE CP y CPS

LLAMA.PE administra los documentos Declaración de Prácticas de Certificación, Política de Seguridad, Política y Plan de Privacidad, y todos los documentos normativos de la EC de LLAMA.PE. Los responsable de aprobar estos documentos es:

Para cualquier consulta contactar:

- Nombre: Ronald Macedo
- Cargo: Responsable de la Entidad de Certificación de LLAMA.PE
- Dirección de correo electrónico: legal@llama.pe
- Teléfono: 01 3012200

11 PUBLICACIÓN DE LA DECLARACIÓN DE PRÁCTICAS

La Declaración de Prácticas de Certificación – CPS y de Registro – RPS de LLAMA.PE, así como la Política de Seguridad, Política y Plan de Privacidad de la Entidad de Certificación y de Registro, y otra documentación relevante son publicadas en la siguiente dirección:

https://llama.pe

Todas las modificaciones relevantes en la documentación de LLAMA.PE, serán comunicadas al INDECOPI y las nuevas versiones del documento serán publicadas en el mismo sitio web.

El presente documento es firmado por el Responsable de la EC de LLAMA.PE antes de ser publicado, y se controlan las versiones del mismo, a fin de evitar modificaciones y suplantaciones no autorizadas.

Las modificaciones relativas a la CPS u otra documentación relativa, serán publicadas luego de ser aprobadas por el INDECOPI.

12 RESPONSABILIDADES SOBRE REPOSITORIOS Y PUBLICACIÓN DE INFORMACIÓN

Certificado Raíz

https://llama.pe/repository

Certificados Subordinadas

https://llama.pe/repository

Lista de Certificados Revocados (CRL)

https://llama.pe/repository

Declaración de Prácticas de Certificación (CPS)

https://llama.pe/repository

12.1 PUBLICACIÓN DE LA INFORMACIÓN DE CERTIFICACIÓN

El Responsable de la EC de LLAMA.PE es el encargado de la autorización de la publicación de la CPS y es responsable de asegurar la integridad y disponibilidad de la información publicada en la página Web: https://llama.pe

La Lista de Certificados Revocados es publicada en la página web de LLAMA.PE y está firmada digitalmente por la Entidad de Certificación LLAMA.PE CA.

12.2 PLAZO O FRECUENCIA DE LA PUBLICACIÓN

- Certificado Raíz

El certificado raíz se publicará y permanecerá en la página Web de la Entidad de Certificación LLAMA.PE, durante todo el tiempo en que se estén prestando servicios de certificación digital.

- Certificado Subordinada

El certificado de la EC Subordinada se publicará y permanecerá en la página Web de la Entidad de Certificación LLAMA.PE, durante todo el tiempo en que se estén prestando servicios de certificación digital.

- Lista de Certificados Revocados (CRL)

La Entidad de Certificación LLAMA.PE, publicará en la página Web, la lista de certificados revocados en los eventos y con la periodicidad definidas en el numeral.

- Declaración de Prácticas de Certificación (CPS)

Con autorización del Responsable de la Entidad de Certificación de LLAMA.PE y el INDECOPI, se publicará la versión finalmente aprobada. Los cambios generados en cada nueva versión serán previamente informados al INDECOPI y publicados en la página Web de La Entidad de Certificación LLAMA.PE junto con la nueva versión. La Auditoría anual validará estos cambios y emitirá el informe de cumplimiento.

12.3 CONTROLES DE ACCESO A LOS REPOSITORIOS

La consulta a los repositorios disponibles en la página Web de La Entidad de Certificación LLAMA.PE, antes mencionados, es de libre acceso al público en general. La integridad y disponibilidad de la información publicada es responsabilidad de La Entidad de Certificación LLAMA.PE, que cuenta con los recursos y procedimientos necesarios para restringir el acceso a los repositorios con otros fines diferentes a la consulta y a la página Web por parte de personas ajenas.

13 IDENTIFICACIÓN Y AUTENTICACIÓN

13.1 NOMBRES

13.1.1 TIPOS DE NOMBRES

Los nombres se distinguen conforme al estándar X.501.

La estructura y el contenido de los campos de cada certificado emitido por LLAMA.PE se encuentran descritos en la sección Perfiles de certificado y CRL.

13.1.2 NECESIDAD DE QUE LOS NOMBRES TENGAN SIGNIFICADO

En los casos en que un producto de LLAMA.PE permite el uso de un rol o nombre de departamento y donde se incluye el campo de OU en el DN, se pueden agregar elementos únicos adicionales al DN dentro del campo de OU para permitir que los terceros que confían diferencien entre los certificados con los Elementos comunes DN. Cabe destacar que, en caso se emitan certificados de prueba se colocará como CN "test".

13.1.3 ANONIMATO Y PSEUDO ANONIMATO DE LOS TITULARES

LLAMA.PE puede emitir Certificados anónimos o seudónimos de entidad final, siempre que dichos códigos no estén prohibidos por la política aplicable y, si es posible, se conserva la singularidad del espacio de nombres.

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. 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.

13.1.4 REGLAS PARA LA INTERPRETACIÓN DE VARIAS FORMAS DE NOMBRE

LLAMA.PE atiende en todo caso a lo marcado por el estándar X.500.

13.1.5 SINGULARIDAD DE LOS NOMBRES

LLAMA.PE no reasigna un nombre a un suscriptor que ya hubiera sido asignado a otro diferente. Para lo cual, la identificación del titular debe estar formada por su nombre y apellidos, más su documento oficial de identidad.

Asimismo, cuando aparezcan datos de personas jurídicas, esta identificación se debe realizar por medio de su denominación o razón social y su RUC. Además del nombre y apellidos del suscriptor, más su documento oficial de identidad.

13.1.6 RECONOCIMIENTO, AUTENTICACIÓN Y PAPEL DE LAS MARCAS RECONOCIDAS.

LLAMA.PE no podrá volver a asignar un nombre de titular que ya haya sido asignado a un titular diferente.

No obstante, LLAMA.PE no se compromete a buscar evidencias acerca de los derechos de uso sobre marcas registradas u otros signos distintivos con anterioridad a la emisión de los certificados.

14 VALIDACIÓN INICIAL DE LA IDENTIDAD

14.1 MÉTODO PARA DEMOSTRAR LA POSESIÓN DE LA CLAVE PRIVADA

El modelo de generación de claves utilizado se indica a continuación:

- Generación de Claves por parte de la EC.

En Software, se entregan al Suscriptor mediante correo a través ficheros protegidos utilizando el Standard PKCS#12. La seguridad del proceso queda garantizada debido a que el código de acceso PKCS#12 que posibilita la instalación de este en las aplicaciones, es entregada por un medio distinto al utilizado en la recepción inicial.

En hardware, la generación de claves se realiza en un dispositivo que cumple el estándar FIPS 140-2 nivel 2 el cual es realizado por personal de Llama.pe con un rol de confianza del correspondiente o personal de la empresa autorizada para realizar dicha actividad..

- Generación de las claves por el Suscriptor

El Suscriptor dispone de un mecanismo de generación de claves en software. La prueba de posesión de la clave privada en estos casos es la petición recibida por la EC en formato PKCS#10.

Las claves privadas serán provistas directamente al suscriptor o al módulo criptográfico del mismo sin generar copias de las mismas.

14.2 AUTENTICACIÓN DE LA IDENTIDAD DE UNA ORGANIZACIÓN (PERSONA JURÍDICA)

La RPS de LLAMA.PE describe específicamente los procedimientos de autenticación, documentación requerida y validación de la identidad de personas jurídicas.

14.3 AUTENTICACIÓN DE LA IDENTIDAD DE UNA IDENTIDAD INDIVIDUAL (CERTIFICADO DE PROFESIONALES)

La RPS de LLAMA.PE describe específicamente los procedimientos de autenticación, documentación requerida y validación de la identidad de profesionales.

14.4 AUTENTICACIÓN DE LA IDENTIDAD DE UNA ORGANIZACIÓN (PERSONA JURÍDICA CON ATRIBUTO)

La RPS de LLAMA.PE describe específicamente los procedimientos de autenticación, documentación requerida y validación de la identidad de suscriptores.

14.5 AUTENTICACIÓN DE LA IDENTIDAD DE UNA ORGANIZACIÓN (PERSONA JURÍDICA AGENTE AUTOMATIZADO)

La RPS de LLAMA.PE describe específicamente los procedimientos de autenticación, documentación requerida y validación de la identidad para certificados de agente automatizado.

14.6 AUTENTICACIÓN DE UNA IDENTIDAD INDIVIDUAL (PERSONA NATURAL)

La RPS de LLAMA.PE describe específicamente los procedimientos de autenticación, documentación requerida y validación de la identidad de personas naturales.

14.7 INFORMACIÓN DE TITULAR NO VERIFICADA

Bajo ninguna circunstancia LLAMA.PE omitirá las labores de verificación que conduzcan a la identificación del Suscriptor y que se traduce en la solicitud de exhibición de los documentos mencionados para organizaciones y personas naturales

14.8 VALIDACIÓN DE LA AUTORIDAD

La validación de la Entidad de Certificación LLAMA.PE respecto a la propiedad de un dominio, se realiza a través de la comprobación de la existencia de un correo que contiene la dirección del dominio en cuestión y/o verificación de datos de registro de dominio respectivo.

Los procedimientos de autenticación y de validación son descritos en el documento de Declaración y Política de Registro de LLAMA.PE.

14.9 CRITERIOS PARA LA INTEROPERABILIDAD

La Entidad de Certificación LLAMA.PE, únicamente emitirá certificados a ER Subordinadas, que estén directamente vinculadas o terceros con vínculo contractual los cuales se someten al cumplimiento de las CP y CPS de la EC Llama.pe.

15 IDENTIFICACIÓN Y AUTENTICACIÓN PARA PETICIONES DE RE-EMISIÓN DE CLAVES

15.1 IDENTIFICACIÓN Y AUTENTICACIÓN PARA RE-EMISIÓN DE RUTINA

LLAMA.PE realiza en todos los eventos del proceso de autenticación del solicitante incluso en los de re-emisión y con base en ello emite los certificados digitales.

Los procedimientos de autenticación son descritos en el documento de Declaración y Política de Registro de LLAMA.PE.

15.2 IDENTIFICACIÓN Y AUTENTICACIÓN TRAS UNA REVOCACIÓN

Debido a que una revocación implica la expedición de un nuevo certificado, LLAMA.PE realiza un nuevo proceso de autenticación del solicitante.

Los procedimientos de autenticación son descritos en el documento de Declaración y Política de Registro de LLAMA.PE.

16 IDENTIFICACIÓN Y AUTENTICACIÓN PARA PETICIONES DE REVOCACIÓN

LLAMA.PE atiende las peticiones de revocación de conformidad con las causales de revocación especificadas en el documento de Declaración y Política de Registro de LLAMA.PE, y autentica la identidad de quien solicita la revocación de certificado.

Los procedimientos de autenticación de la identidad de los titulares y suscriptores son descritos en la RPS de LLAMA.PE.

17 REQUISITOS OPERACIONALES PARA EL TIEMPO DE VIDA DE LOS CERTIFICADOS

17.1 SOLICITUD DEL CERTIFICADO

Dicho procedimiento le compete a la Entidad de Registro y por lo tanto se describe en el documento Declaración y Política de Registro de LLAMA.PE.

17.2 QUIÉN PUEDE SOLICITAR UN CERTIFICADO

Los procedimientos relativos a la Entidad de Registro son descritos en el documento de Declaración y Política de Registro de LLAMA.PE.

17.3 PROCESO DE REGISTRO Y RESPONSABILIDADES

Los procedimientos relativos a la Entidad de Registro son descritos en el documento de Declaración y Política de Registro de LLAMA.PE.,

18 TRAMITACIÓN DE SOLICITUD DE CERTIFICADOS

18.1 REALIZACIÓN DE LAS FUNCIONES DE IDENTIFICACIÓN Y AUTENTICACIÓN

Los procedimientos relativos a la Entidad de Registro son descritos en el documento de Declaración y Política de Registro LLAMA.PE.

18.2 APROBACIÓN O RECHAZO DE LAS SOLICITUDES DE CERTIFICADO

Los procedimientos relativos a la Entidad de Registro son descritos en el documento de Declaración y Política de Registro de LLAMA.PE.

18.3 PLAZO PARA PROCESAR LAS SOLICITUDES DE CERTIFICADO

Los procedimientos relativos a la Entidad de Registro son descritos en el documento de Declaración y Política de Registro de LLAMA.PE – RPS.

19 EMISIÓN DE CERTIFICADOS

19.1 ACTUACIONES DE LA EC DURANTE LA EMISIÓN DE CERTIFICADOS

Una vez aprobada la solicitud se procederá a la emisión del certificado, que deberá ser entregado de forma segura al Suscriptor. Contamos con 3 casos en los que un certificado digital puede ser emitido:

19.1.1 EMISIÓN DE CERTIFICADO MEDIANTE SOFTWARE (.pfx o .p12)

- La Entidad de Certificación recibe la solicitud de la Entidad de Registro asociada una vez que la validación de identidad fue completada correctamente.
- El Operador de Registro aprueba la solicitud usando su firma digital.
- El solicitante recibe el enlace de descarga del certificado en el correo electrónico indicado en el pedido.

19.1.2 EMISIÓN DE CERTIFICADO MEDIANTE HARDWARE

- La Entidad de Certificación recibe la solicitud de la Entidad de Registro asociada una vez que la validación de identidad fue completada correctamente.
- El Operador de Registro aprueba la solicitud usando su firma digital.
- El certificado se instala directamente en el dispositivo criptográfico del solicitante usando Internet Explorer mediante el formato PKCS#10.

19.1.3 EMISIÓN DE CERTIFICADO MEDIANTE WATANA APP

- La Entidad de Certificación recibe la solicitud de la Entidad de Registro asociada una vez que la validación de identidad fue completada correctamente.
- El Operador de Registro aprueba la solicitud usando su firma digital.
- El solicitante recibe un enlace de descarga del certificado en el correo electrónico indicado en el pedido. Allí se generará un QR el cual debe ser escaneado usando Watana app. En ese momento, el certificado digital será generado en el almacén de claves del celular del solicitante. Para este caso la ER no administra ningún módulo criptográfico ya que el certificado es generado en el almacén de claves del celular del usuario.

19.2 NOTIFICACIÓN AL SUSCRIPTOR POR LA EC DE LA EMISIÓN DEL CERTIFICADO

La EC de LLAMA.PE notificará al Suscriptor la emisión del certificado y el método de descarga si es necesario.

20 ACEPTACIÓN DEL CERTIFICADO

20.1 FORMA EN LA QUE SE ACEPTA EL CERTIFICADO

El certificado se considera aceptado una vez que es descargado. La EC de Llama.pe cuenta con un mecanismo para saber cuándo es que el certificado digital es descargado a fin de dar la conformidad correspondiente.

Por otro lado, el titular/suscriptor puede dar a conocer su inconformidad con algún dato del perfil del certificado digital a través de un medio no repudiable como un correo electrónico o documentos firmados digitalmente, por ejemplo.

20.2 PUBLICACIÓN DEL CERTIFICADO POR LA EC

Los procedimientos relativos a la Entidad de Registro son descritos en el documento de Declaración y Política de Registro de LLAMA.PE.

20.3 NOTIFICACIÓN DE LA EMISIÓN DEL CERTIFICADO POR LA EC A OTRAS ENTIDADES

La EC de Llama.pe notifica sobre la emisión de un certificado digital a través de la plataforma de la ER de Llama.pe.

21 USO DE LA CLAVE PRIVADA Y DEL CERTIFICADO

21.1 USO DE LA CLAVE PRIVADA Y DEL CERTIFICADO POR EL TITULAR/SUSCRIPTOR

Los suscriptores deben proteger su clave privada teniendo cuidado de evitar la divulgación a terceros. El contrato de Suscriptor identifica las obligaciones del Suscriptor con respecto a la Protección de Clave Privada (para más información, revisar el documento: ER-DPR-001 DECLARACIÓN Y POLÍTICA DE REGISTRO). Las claves privadas sólo se deben utilizar como se especifica en los campos de uso de clave y de uso extendido de clave como se indica en el Certificado correspondiente. Donde es posible hacer una copia de seguridad de una clave privada, los suscriptores deben utilizar el mismo nivel de cuidado y protección atribuido a la clave privada en vivo. Al final de la vida útil de una clave privada, los suscriptores deben eliminar de forma segura la clave privada y los fragmentos que se han dividido para fines de copia de seguridad.

21.2 USO DE LA CLAVE PRIVADA Y DEL CERTIFICADO POR TERCEROS QUE CONFÍAN

Es responsabilidad de los terceros que confían, verificar el estado del certificado. Asimismo, podrán utilizar los certificados para aquello que establece la presente CPS y la Política de Certificación.

22 RE-EMISIÓN DEL CERTIFICADO SIN CAMBIO DE CLAVES

La EC de LLAMA.PE no permite la re-emisión de certificados sin renovación de claves.

23 RE-EMISIÓN DEL CERTIFICADO CON CAMBIO DE CLAVES

Para la Entidad de Certificación de LLAMA.PE, un requerimiento de re-emisión de un certificado con cambio de claves es un requerimiento normal de solicitud de un certificado digital como si fuera uno nuevo y por consiguiente implica el cambio de claves y así lo reconoce y acepta el solicitante.

La EC de LLAMA.PE comunicará al suscriptor, con una anticipación de al menos 30 días antes de la expiración del certificado, para que pueda renovar a tiempo dicho certificado. Si el suscriptor no solicita la re-emisión de certificado, el certificado expirará. Luego de ello, el suscriptor deberá realizar el proceso de validación de identidad desde la etapa inicial.

23.1 CIRCUNSTANCIAS PARA LA RE-EMISIÓN DE CERTIFICADOS CON CAMBIO DE CLAVES

Las circunstancias son definidas en la Declaración y Política de Registro de LLAMA.PE como Entidad de Registro.

23.2 QUIÉN PUEDE SOLICITAR UNA RE-EMISIÓN CON CAMBIO DE CLAVES.

Las precisiones sobre quién puede solicitar una re-emisión son definidas en la Declaración y Política de Registro de LLAMA.PE como Entidad de Registro.

23.3 TRÁMITES PARA LA SOLICITUD DE RE-EMISIÓN DE CERTIFICADOS CON CAMBIO DE CLAVES.

El procedimiento para re-emisión de certificados digitales es definido en la Declaración y Política de Registro de LLAMA.PE como Entidad de Registro.

23.4 NOTIFICACIÓN AL TITULAR DE LA EMISIÓN DE UN NUEVO CERTIFICADO CON CAMBIO DE CLAVES

El procedimiento para re-emisión de certificados digitales es definido en la Declaración y Política de Registro de LLAMA.PE como Entidad de Registro.

23.5 FORMA EN LA QUE SE ACEPTA LA RE-EMISIÓN DE UN CERTIFICADO

El procedimiento para re-emisión de certificados digitales es definido en la Declaración y Política de Registro de LLAMA.PE como Entidad de Registro.

23.6 PUBLICACIÓN DEL CERTIFICADO RE-EMITIDO POR LA EC

El procedimiento para re-emisión de certificados digitales es definido en la Declaración y Política de Registro de LLAMA.PE como Entidad de Registro.

23.7 NOTIFICACIÓN DE LA EMISIÓN DE UN CERTIFICADO RE-EMITIDO POR LA EC A OTRAS ENTIDADES

El procedimiento para re-emisión de certificados digitales es definido en la Declaración y Política de Registro de LLAMA.PE como Entidad de Registro.

24 MODIFICACIÓN DE CERTIFICADOS

La modificación del certificado se define como la producción de un nuevo certificado que tiene detalles que difieren de un certificado previamente emitido. LLAMA.PE trata la modificación de la misma manera que la emisión de un nuevo certificado.

25 REVOCACIÓN Y SUSPENSIÓN DE CERTIFICADOS

25.1 CIRCUNSTANCIAS PARA LA REVOCACIÓN DE UN CERTIFICADO

Como mínimo, las causas de revocación de un certificado son debido a:

- Exposición, puesta en peligro o uso indebido de la clave privada.
- Deterioro, alteración o cualquier otro hecho u acto que afecte la clave privada.

- Revocación de las facultades de representación y/o poderes de sus representantes legales o apoderados.
- Cuando la información contenida en el certificado ya no resulte correcta.
- Cuando el suscriptor deja de ser miembro de la comunidad de interés o se sustrae de aquellos intereses relativos a la EC.
- Cuando el suscriptor o titular incumple las obligaciones a las que se encuentra comprometido dentro de la IOFE a través de lo estipulado en el contrato del suscriptor y/o titular.
- Cuando la información contenida en el certificado ya no resulte correcta.
- Decisión de la legislación respectiva.
- Falta de pago del certificado.
- La incapacidad sobrevenida o la muerte del Firmante o responsable del certificado.
- Resolución de la autoridad administrativa o judicial competente.

25.2 QUIÉN PUEDE SOLICITAR UNA REVOCACIÓN

La revocación de un certificado podrá solicitarse por:

- El Suscriptor.
- La Entidad (a través de un representante de la misma).
- La ER o la EC. Adicionalmente las que marquen las políticas de certificación concretas.
- Otro tercero que tenga evidencia de alguna circunstancia de revocación previamente mencionada.

25.3 PROCEDIMIENTO DE SOLICITUD DE REVOCACIÓN

El procedimiento para revocación de certificados digitales es definido en la Declaración de Prácticas de Registro de LLAMA.PE como Entidad de Registro.

25.4 PERIODO DE GRACIA DE SOLICITUD DE REVOCACIÓN

No aplica.

25.5 PLAZO EN EL QUE LA EC DEBE RESOLVER LA SOLICITUD DE REVOCACIÓN

Los procedimientos relativos a la Entidad de Certificación son descritos en el documento de Declaración y Política de Registro de LLAMA.PE.

25.6 REQUISITOS DE VERIFICACIÓN DE LAS REVOCACIONES POR LOS TERCEROS QUE CONFÍAN

Los procedimientos relativos a la Entidad de Certificación son descritos en el documento de Declaración y Política de Registro de LLAMA.PE.

25.7 FRECUENCIA DE EMISIÓN DE LAS CRLS

La frecuencia de actualización de la CRL es diaria. La frecuencia de actualización de la ARL es cada seis (06) meses.

25.8 TIEMPO MÁXIMO DE LATENCIA DE LAS CRLS

El tiempo entre la generación y publicación de la CRL es menor a una (1) hora, tal como lo establece el INDECOPI.

25.9 DISPONIBILIDAD DE VERIFICACIÓN DEL ESTADO

La información relativa a la CRL estará disponible en línea con un mínimo de 99% anual y un tiempo programado de inactividad máximo de 0.5% anual.

25.10 REQUISITOS DE COMPROBACIÓN DE LA REVOCACIÓN ON-LINE

Para el uso de servicio de la CRL de LLAMA.PE, se debe tener en cuenta que esta Lista se encuentre firmada por LLAMA.PE CA y que sea la última Lista emitida.

25.11 OTRAS FORMAS DISPONIBLES DE DIVULGACIÓN DE INFORMACIÓN DE REVOCACIÓN

No aplica

25.12 REQUISITOS ESPECIALES DE RENOVACIÓN DE CLAVES COMPROMETIDAS

LLAMA.PE utilizará métodos comercialmente razonables para informar a los suscriptores de que su Clave Privada puede haber sido comprometida. Esto incluye los casos en los que se pudieran descubrir nuevas vulnerabilidades.

25.13 CIRCUNSTANCIAS PARA LA SUSPENSIÓN

LLAMA.PE no brinda el servicio de suspensión de certificados digitales, únicamente revocación.

25.14 QUIÉN PUEDE SOLICITAR LA SUSPENSIÓN

LLAMA.PE no brinda el servicio de suspensión de certificados digitales, únicamente revocación.

25.15 PROCEDIMIENTO DE SOLICITUD DE SUSPENSIÓN

LLAMA.PE no brinda el servicio de suspensión de certificados digitales, únicamente revocación.

25.16 LÍMITES DEL PERIODO DE SUSPENSIÓN

LLAMA.PE no brinda el servicio de suspensión de certificados digitales, únicamente revocación.

25.17 NOTIFICACIÓN DE LA REVOCACIÓN DE UN CERTIFICADO

La notificación de la revocación de un certificado digital es enviada directamente al correo electrónico brindado por el solicitante.

26 SERVICIOS DE INFORMACIÓN DEL ESTADO DE CERTIFICADOS

26.1 CARACTERÍSTICAS OPERACIONALES

A fin de contar con un servicio que permita validar si un certificado digital se encuentra revocado, LLAMA.PE cuenta con una CRL que publica desde su página web, sin restricciones de acceso.

26.2 DISPONIBILIDAD DEL SERVICIO

LLAMA.PE cuenta con una disponibilidad de la CRL con un mínimo de 99% anual y un tiempo programado de inactividad máximo de 0.5% anual.

27 CONTROLES FÍSICOS DE LA INSTALACIÓN, GESTIÓN Y OPERACIONALES

27.1 CONTROLES FÍSICOS DE LA INFRAESTRUCTURA TECNOLÓGICA

LLAMA.PE, mantiene políticas de seguridad física y ambiental para los sistemas utilizados para la emisión y gestión de certificados que abarcan el control de acceso físico, protección contra desastres naturales, factores de seguridad contra incendios, fallas en las utilidades de apoyo (por ejemplo, energía, telecomunicaciones), colapso de estructuras y la recuperación de desastres. Los controles deben ser implementados para evitar la pérdida, daño o compromiso de los activos y la interrupción de las actividades empresariales y el robo de la información y las instalaciones de procesamiento de la información. Asimismo, asegura que la infraestructura tecnológica será escalable de acuerdo con el crecimiento del volumen de los aplicativos de sus clientes.

27.1.1 UBICACIÓN FÍSICA Y CONSTRUCCIÓN

Las instalaciones subcontratadas por LLAMA.PE están construidas en un local lo suficientemente alejado donde no pueda ser afectado por amenazas de aniego, incendio, disturbios o atentados terroristas. La estructura es de concreto armado, reforzado con material de atenuación a ondas expansivas.

27.1.2 ACCESO FÍSICO

El acceso físico a las dependencias de LLAMA.PE donde se llevan a cabo procesos de certificación, cuenta con un sistema de control de ingreso, mediante tarjetas de proximidad, también mantiene un registro detallado de acceso al Data Center por personal autorizado, asimismo, cuenta con cámaras de video vigilancia en las áreas de acceso al Data Center, y por último, cuenta con un servicio de seguridad que opera las 24 horas del día para el control de acceso a las instalaciones del Data Center y monitoreo de las cámaras de video-vigilancia.

27.1.3 ALIMENTACIÓN ELÉCTRICA Y AIRE ACONDICIONADO

El control de acceso físico a las dependencias subcontratadas por LLAMA.PE es a través de tarjetas de proximidad y es administrado de forma local. Se controlan todos los accesos tanto de ingresos como de salidas de los empleados, clientes, contratistas y visitantes.

27.1.4 EXPOSICIÓN AL AGUA

Las instalaciones subcontratadas por LLAMA.PE cuentan con un edificio seco, es decir, no cuenta con sistemas de agua ni desagüe para servicios generales. Cuenta con cañerías y drenajes exclusivos para el sistema de Aire Acondicionado de precisión, asimismo es importante mencionar que no cuenta con baños, tanque elevado de agua ni torre de agua de refrigeración de los sistemas de AA de confort de las instalaciones del edificio Administrativo.

27.1.5 PREVENCIÓN Y PROTECCIÓN DE INCENDIOS

Todas las paredes de las instalaciones subcontratadas por LLAMA.PE, fueron diseñadas y construidas para retardar la propagación del fuego.

27.1.6 SISTEMA DE ALMACENAMIENTO

Cada medio de almacenamiento se mantiene solo al alcance de personal autorizado

27.1.7 ELIMINACIÓN DEL MATERIAL DE ALMACENAMIENTO DE LA INFORMACIÓN

Cuando deje de ser útil, la información sensible es destruida en la forma más adecuada al soporte que la contenga, de tal manera que la información sea irrecuperable.

27.1.8 BACKUP FUERA DE LA INSTALACIÓN

LLAMA.PE realiza una copia de seguridad de las claves de la EC, manteniendo en todo momento el alcance a personal autorizado y con controles de seguridad.

27.2 CONTROLES DE PROCEDIMIENTO

27.2.1 ROLES DE CONFIANZA

LLAMA.PE, garantiza que todo el personal de confianza es el descrito a continuación y que garantiza una segregación de funciones que disemina el control y limita el fraude interno, no permitiendo que una sola persona controle de principio a fin todas las funciones de certificación, y con una concesión de mínimo privilegio, cuando sea posible.

Los roles de confianza que intervienen en el ciclo de vida de LLAMA.PE son los siguientes:

- Responsable de la EC
- Administrador del sistema operativo
- Administrador de la aplicación de AC
- Titulares de las claves
- Oficial de seguridad y privacidad
- Auditor interno

27.2.2 NÚMERO DE PERSONAS REQUERIDAS POR TAREA

LLAMA.PE garantiza al menos dos personas para realizar las tareas clasificadas como sensibles. Principalmente en la manipulación del dispositivo de custodia de las claves de EC Raíz y EC Subordinadas.

Las personas asignadas para cada rol son identificadas por el Administrador del sistema operativo que se asegurará que cada persona realiza las operaciones para las que está asignado. Cada persona solo controla los activos necesarios para su rol, asegurando así que ninguna persona accede a recursos no asignados. El acceso a recursos se realiza dependiendo del activo mediante tarjetas criptográficas y PINs.

27.3 CONTROLES DE PERSONAL

27.3.1 REQUISITOS SOBRE LA CUALIFICACIÓN, EXPERIENCIA Y CONOCIMIENTO PROFESIONALES

Todo el personal que realiza tareas calificadas como confiables, lleva al menos un año trabajando para la EC y tiene contratos laborales fijos. Todo el personal está cualificado y ha sido instruido convenientemente para realizar las operaciones que le han sido asignadas. El personal en puestos de confianza se encuentra libre de intereses personales que entran en conflicto con el desarrollo de la función que tenga encomendada.

27.3.2 PROCEDIMIENTO DE COMPROBACIÓN DE ANTECEDENTES

El área encargada de Recursos Humanos de LLAMA.PE se encarga de realizar las investigaciones pertinentes antes de la contratación de cualquier persona. LLAMA.PE nunca asigna tareas confiables a personal con al menos una antigüedad de un año.

Asimismo el personal de confianza ha sido sometido a verificación de antecedentes penales y policiales.

27.3.3 REQUISITOS DE FORMACIÓN

El personal encargado de tareas de confianza ha sido y será formado de acuerdo al plan de formación.

El plan de formación incluye los siguientes contenidos:

- Principios y mecanismos de seguridad de la jerarquía pública de certificación.
- Versiones de hardware y aplicaciones en uso.
- Tareas que debe realizar la persona.
- Gestión y tramitación de incidentes y compromisos de seguridad.
- Procedimientos de continuidad de negocio y emergencia.
- Procedimiento de gestión y de seguridad en relación con el tratamiento de los datos de carácter personal.

27.3.4 REQUISITOS Y FRECUENCIA DE ACTUALIZACIÓN DE FORMACIÓN

LLAMA.PE realiza los cursos de actualización necesarios para asegurarse de la correcta realización de las tareas de certificación, especialmente cuando se realicen modificaciones sustanciales en las mismas.

27.3.5 FRECUENCIA Y SECUENCIA DE ROTACIÓN DE TAREAS

No está estipulado.

27.3.6 SANCIONES POR ACTUACIONES NO AUTORIZADAS

Cuando un empleado realice acciones no autorizadas, LLAMA.PE tiene la potestad de sancionarlo o incluso ser retirado de la empresa. La decisión será tomada por el Responsable de la EC de LLAMA.PE.

27.3.7 REQUISITOS DE CONTRATACIÓN DE TERCEROS

Los empleados contratados para realizar tareas confiables firman anteriormente las cláusulas de confidencialidad y los requerimientos operacionales empleados por LLAMA.PE. Cualquier acción que comprometa la seguridad de los procesos aceptados podría una vez evaluados dar lugar al cese del contrato laboral. En el caso de que todos o parte de los servicios de certificación sean operados por un tercero, los controles y previsiones realizadas en esta sección, o en otras partes de la CPS, serán aplicados y cumplidos por el tercero que realice las funciones de operación de los servicios de certificación, la entidad de certificación será responsable en todo caso de la efectiva ejecución. Estos aspectos quedan concretados en el instrumento jurídico utilizado para acordar la prestación de los servicios de certificación por tercero distinto de LLAMA.PE debiendo obligarse los terceros a cumplir con los requerimientos exigidos por LLAMA.PE.

27.3.8 DOCUMENTACIÓN PROPORCIONADA AL PERSONAL

LLAMA.PE, pone a disposición de todo el personal la documentación donde se detallen las funciones encomendadas, en particular la normativa de seguridad y la CPS.

Esta documentación se encuentra en un repositorio interno accesible por cualquier empleado de LLAMA.PE, en el repositorio existe una lista de documentos de obligado conocimiento y cumplimiento. Adicionalmente se suministrará la documentación que precise el personal en cada momento, al objeto de que pueda desarrollar de forma competente sus funciones.

27.4 PROCEDIMIENTOS DE CONTROL DE SEGURIDAD

A fin de garantizar una correcta gestión de la seguridad en los sistemas de información, LLAMA.PE lleva a cabo los controles descritos a continuación.

27.4.1 TIPOS DE EVENTOS REGISTRADOS

Se registra y guarda los registros de auditoría de todos los eventos relativos al sistema de seguridad de la EC.

Se registrarán los siguientes eventos:

- Encendido y apagado del sistema.
- Intentos de creación, borrado, establecimiento de contraseñas o cambio de privilegios.

- Intentos de inicio y fin de sesión.
- Intentos de accesos no autorizados al sistema de la EC a través de la red.
- Intentos de accesos no autorizados al sistema de archivo.
- Acceso físico a los registros de auditoría.
- Cambios en la configuración y mantenimiento del sistema.
- Registros de las aplicaciones de la EC.
- Encendido y apagado de la aplicación de la EC.
- Cambios en los detalles de la EC y/o sus claves.
- Cambios en la creación de políticas de certificados.
- Generación de claves propias.
- Creación y revocación de certificados.
- Registros de la destrucción de los medios que contienen las claves, datos de Activación.
- Eventos relacionados con el ciclo de vida del módulo criptográfico, como recepción, uso y desinstalación.

27.4.2 PERIODO DE RETENCIÓN DE LOS REGISTROS DE AUDITORÍA

LLAMA.PE almacena la información de los registros de auditoría al menos durante diez (10) años. Llama.pe almacena la información de acuerdo a la Guía de Acreditación de INDECOPI.

27.4.3 PROTECCIÓN DE LOS REGISTROS DE AUDITORÍA

Los registros de auditoría se protegen mediante control de acceso. Solo el Administrador del Sistema de la EC tiene la posibilidad de acceder a los mismos.

27.4.4 PROCEDIMIENTOS DE BACKUP DE LOS REGISTROS DE AUDITORÍA

Diariamente se genera un respaldo de todos los servicios y sistemas de la EC de LLAMA.PE.

27.4.5 SISTEMA DE RECOGIDA DE INFORMACIÓN DE AUDITORÍA (INTERNA O EXTERNA)

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

27.4.6 NOTIFICACIÓN AL SUJETO CAUSA DEL EVENTO

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

27.4.7 ANÁLISIS DE VULNERABILIDADES

El análisis de vulnerabilidades queda cubierto por los procesos de auditoría de LLAMA.PE. Anualmente se revisan los procesos de gestión de riesgos y vulnerabilidades dentro del marco de revisión de la acreditación de INDECOPI.

LLAMA.PE corrige cualquier problema reportado y es registrado por el Oficial de Seguridad.

27.5 ARCHIVO DE REGISTROS

27.5.1 TIPOS DE EVENTOS ARCHIVADOS

Los siguientes documentos implicados en el ciclo de vida del certificado son almacenados por la EC o por las ERs:

- Todos los datos relativos a los certificados, incluyendo los contratos de suscriptor/titular.
- Los datos relativos a su identificación.
- Solicitudes de emisión y revocación de certificados.

- Estado de acreditación.
- Tipo de documento presentado en la solicitud del certificado.
- Número de identificación único proporcionado por el documento anterior.
- Todos los certificados emitidos o publicados.
- Claves públicas de la EC.
- El registro de auditorías.
- Políticas y Prácticas de Certificación.

LLAMA.PE responsable del correcto archivo de todo este material. En cuanto al ciclo de vida de su certificado, la EC debe registrar lo siguiente:

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

En cuanto al ciclo de vida de los dispositivos criptográficos, la EC debe registrar lo siguiente:

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

En cuanto ciclo de vida de las claves del suscriptor, la EC debe registrar lo siguiente:

- Generación de las claves
- Distribución de las claves (si fuera aplicable)
- Archivo de las claves (si fuera aplicable)
- Destrucción de las claves
- Identidad de la entidad que autoriza las operaciones de gestión de las claves
- Compromiso de las claves

La EC debe registrar o requerir a la ER el registro de la siguiente información para la solicitud de certificados:

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

La EC debe registrar los siguientes eventos sensibles con respectos a la seguridad:

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

27.5.2 PERIODO DE CONSERVACIÓN

Los certificados, los contratos con los suscriptores y cualquier información indicada en el apartado Tipos de eventos archivados, serán conservados durante al menos diez (10) años.

27.5.3 PROTECCIÓN DE ARCHIVOS

Las medidas de seguridad que se utilizan para garantizar la confidencialidad de los datos proporcionados por los suscriptores y los titulares comprenden la asignación de personal cualificado para su tratamiento y el almacenamiento en cajas de seguridad ignífugas e instalaciones externas.

27.5.4 PROCEDIMIENTOS DE BACKUP DEL ARCHIVO DE REGISTROS

LLAMA.PE realiza copias de respaldo anuales de todos sus documentos electrónicos.

27.5.5 REQUISITOS PARA EL SELLADO DE TIEMPO DE LOS REGISTROS

No aplica.

27.5.6 SISTEMA DE ARCHIVO DE LA INFORMACIÓN DE AUDITORÍA (INTERNA O EXTERNA)

LLAMA.PE cuenta con un documento que describe el procedimiento de gestión de registros de auditoría.

27.5.7 PROCEDIMIENTOS PARA OBTENER Y VERIFICAR INFORMACIÓN ARCHIVADA.

LLAMA.PE dispone de un documento de seguridad informática donde se describe el proceso para verificar que la información archivada es correcta y accesible.

27.6 CAMBIO DE CLAVES DE UNA EC

El cambio de claves de entidad final es realizado mediante la realización de un nuevo proceso de emisión (ver apartado correspondiente de esta CPS).

27.7 RECUPERACIÓN EN CASO DE COMPROMISO DE UNA CLAVE Y DESASTRE NATURAL U OTRO TIPO DE CATÁSTROFE

La EC de LLAMA.PE ha desarrollado un Plan de continuidad, el cual contempla el compromiso de la clave raíz de la EC como un caso particular. Esta incidencia afecta, en caso de sustitución de las claves, a los reconocimientos por diferentes aplicativos del sector privado y público.

27.8 CESE DE UNA EC O ER

27.8.1 CESE DE LA EC DE LLAMA.PE

Antes del cese de su actividad LLAMA.PE realizará las siguientes actuaciones:

- Proveerá de los fondos necesarios, mediante carta fianza, para continuar la finalización de las actividades de revocación.
- Informará a los suscriptores, titulares y terceros que confían del cese con por lo menos treinta (30) días calendario de anticipación.
- Transferirá sus obligaciones relativas al mantenimiento de la información de registro y de los registros de auditoría durante el periodo de tiempo indicado en la CPS.
- Las claves privadas de la EC serán destruidas o deshabilitadas para su uso.
- LLAMA.PE mantendrá los certificados activos y el sistema de verificación y revocación hasta la extinción de todos los certificados emitidos.
- Todas estas actividades estarán recogidas en detalle en el Plan de continuidad de LLAMA.PE.

27.8.2 CESE DE LA ER DE LLAMA.PE

Antes de su finalización, la ER de LLAMA.PE informará al INDECOPI, a los suscriptores, titulares y terceros que confían sobre el cese de sus operaciones con por lo menos treinta (30) días calendario de anticipación.

Las demás especificaciones están descritas en la Política de Seguridad EC de Llama.pe.

28 CONTROLES TÉCNICOS DE SEGURIDAD

28.1 GENERACIÓN E INSTALACIÓN DEL PAR DE CLAVES

28.1.1 GENERACIÓN DEL PAR DE CLAVES DE LA EC

La EC deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que las claves de la EC sean generadas de acuerdo a los estándares.

En particular:

1. La generación de la clave de la EC se realizará en un entorno asegurado físicamente por el personal adecuado según los roles de confianza y, al menos, con un control dual. El personal autorizado para desempeñar estas funciones estará limitado a aquellos requerimientos desarrollados en la CPS
2. La generación de la clave de la EC se realizará en un dispositivo que cumpla los requerimientos que se detallan en el FIPS 140-2, en su nivel 3.

28.1.2 GENERACIÓN DEL PAR DE CLAVES DEL SUSCRIPTOR

El par de claves será generado por el emisor o bajo su control.

Si las claves del suscriptor/titular son generadas por la EC, ésta deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que las claves son generadas de forma segura y que se mantendrá la privacidad de las mismas. En particular:

1. Las claves serán generadas usando un algoritmo adecuado para los propósitos de la firma electrónica avanzada.
2. Las claves tendrán una longitud de clave adecuada para los propósitos de la firma electrónica avanzada y para el algoritmo de clave pública empleado.
3. Las claves serán generadas y guardadas de forma segura antes de entregárselas al suscriptor/titular.
4. Las claves serán destruidas de forma segura después de su entrega al suscriptor/titular.

28.1.3 ENTREGA DE LA CLAVE PRIVADA AL SUSCRIPTOR

Cuando la clave privada del suscriptor/titular sea generada por la EC, ésta le será entregada de manera que la confidencialidad de la misma no sea comprometida y sólo el suscriptor/titular tenga acceso a la misma.

La clave privada deberá ser almacenada en todo caso en un dispositivo seguro de almacenamiento de los datos de creación de firma (DSADCF) o en dispositivo seguro de creación de firma (DSCF).

Así mismo, este dispositivo seguro podrá consistir en un medio de almacenamiento externo (p. ej. smartcard o key token) o bien en un medio software (p. ej. PKCS10).

Cuando la EC entrega un dispositivo seguro al suscriptor/titular, deberá hacerlo de forma segura. En particular:

1. La preparación del dispositivo seguro, deberá ser controlada de manera segura por la EC.
2. El dispositivo seguro será guardado y distribuido de forma segura.
3. Cuando el dispositivo seguro tenga asociado unos datos de activación de Tercero que confía (p.ej. un código PIN), los datos de activación se deberán preparar de forma segura y distribuirse de manera separada del dispositivo seguro de creación de firma.

28.1.4 ENTREGA DE LA CLAVE PÚBLICA DEL SUSCRIPTOR AL EMISOR DEL CERTIFICADO

Cuando el Suscriptor pueda generar sus propias claves, la clave pública del Suscriptor tiene que ser transferida a la ER o EC, de forma que se asegure que

- No ha sido cambiado durante el traslado,
- El remitente está en posesión de la clave privada que se corresponde con la clave pública transferida y
- El proveedor de la clave pública es el legítimo Tercero que confía que aparece en el certificado.

28.1.5 ENTREGA DE LA CLAVE PÚBLICA DE LA EC A LOS TERCEROS QUE CONFÍAN

La EC deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que la integridad y la autenticidad de la clave pública de la EC y los parámetros a ella asociados son mantenidos durante su distribución a los Terceros que confían. En particular:

1. La clave pública de la EC estará disponible a los Terceros que confían de manera que se asegure la integridad de la clave y se autentique su origen.
2. El certificado de la EC y su fingerprint (huella digital) estarán a disposición de los Terceros que confían a través de su página web.

28.1.6 TAMAÑO Y PERIODO DE VALIDEZ DE LAS CLAVES DEL EMISOR

El emisor deberá usar claves basadas en el algoritmo RSA con una longitud mínima de 2048 bits para firmar certificados, en todo caso estará sujeto en este aspecto a la práctica habitual en esta tecnología.

El periodo de uso de una clave privada será como máximo de 3 años, después del cual deberán cambiarse estas claves.

El periodo de validez del certificado de la EC se establecerá como mínimo en atención a lo siguiente:

- El periodo de uso de la clave privada de la EC,
- El periodo máximo de validez de los certificados de los Suscriptores firmados con esa clave.

28.1.7 TAMAÑO Y PERIODO DE VALIDEZ DE LAS CLAVES DEL SUSCRIPTOR

El Suscriptor deberá usar claves basadas en el algoritmo RSA con una longitud mínima de 2048 bits, en todo caso estará sujeto en este aspecto a la práctica habitual en esta tecnología.

El periodo de uso de la clave pública y privada del Suscriptor no deberá ser superior a 3 años y no excederá del periodo durante el cual los algoritmos de criptografía aplicada y sus parámetros correspondientes dejan de ser criptográficamente fiables.

28.1.8 HARDWARE/SOFTWARE DE GENERACIÓN DE CLAVES

Las claves de la EC deberán ser generadas en un módulo criptográfico validado al menos por el nivel 2 de FIPS 140-1 o por un nivel de funcionalidad y seguridad equivalente.

El par de claves y las claves simétricas para los Suscriptores serán generadas en un módulo de software y / o hardware criptográfico.

28.1.9 FINES DEL USO DE LA CLAVE

La EC deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que las claves de firma de la EC son usadas sólo para los propósitos de generación de certificados y para la firma de CRLs.

La clave privada del Suscriptor deberá ser usada únicamente para la generación de firmas electrónicas avanzadas, de acuerdo con el apartado Ámbito de aplicación y usos.

28.2 PROTECCIÓN DE LA CLAVE PRIVADA

La EC deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que las claves privadas de la EC continúan siendo confidenciales y mantienen su integridad. En particular:

1. La clave privada de firma de la EC será almacenada y usada en un dispositivo criptográfico seguro, el cual cumple los requerimientos que se detallan en el FIPS 140-2, en su nivel 3.
2. Cuando la clave privada de la EC esté fuera del módulo criptográfico esta deberá estar cifrada
3. Se deberá hacer un back up de la clave privada de firma de la EC, que deberá ser almacenada y recuperada sólo por el personal autorizado según los roles de confianza, usando, al menos un control dual en un medio físico seguro. El personal autorizado para desempeñar estas funciones estará limitado a aquellos requerimientos desarrollados en la CPS
4. Las copias de back up de la clave privada de firma de la EC se regirán por el mismo o más alto nivel de controles de seguridad que las claves que se usen en ese momento.

Del suscriptor/titular

La EC deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que la clave privada está protegida de forma que:

- El suscriptor/titular pueda mantener la clave privada bajo su exclusivo control.
- Su secreto está razonablemente asegurado.
- La clave privada puede ser efectivamente protegida por el suscriptor/titular contra un uso ajeno

28.3 ESTÁNDARES PARA MÓDULOS CRIPTOGRÁFICOS

Todas las operaciones criptográficas deben ser desarrolladas en un módulo validado por al menos el nivel 2 de FIPS 140-2 o por un nivel de funcionalidad y seguridad equivalente.

28.3.1 CONTROL MULTIPERSONA (N DE M) DE LA CLAVE PRIVADA

Se requerirá un control multipersona para la activación de la clave privada de la EC. Este control deberá ser definido adecuadamente por la CPS en la medida en que no se trate de información confidencial o pueda comprometer de algún modo la seguridad del sistema.

28.3.2 CUSTODIA DE LA CLAVE PRIVADA

La clave privada de la EC debe ser almacenada en un medio seguro protegido criptográficamente y al menos bajo un control dual.

Las claves de los Suscriptores estarán custodiadas por este en dispositivos software.

28.3.3 BACKUP DE LA CLAVE PRIVADA

La EC deberá realizar una copia de back up de su propia clave privada que haga posible su recuperación en caso de desastre o de pérdida o deterioro de la misma de acuerdo con el apartado anterior.

Las copias de las claves privadas de los Suscriptores se regirán por lo dispuesto en el punto anterior.

28.3.4 ARCHIVO DE LA CLAVE PRIVADA

La clave privada de la EC no podrá ser archivada una vez finalizado su ciclo de vida. Las claves privadas de Suscriptor no pueden ser archivadas por la EC salvo aquellas usadas para cifrado de datos.

28.3.5 INTRODUCCIÓN DE LA CLAVE PRIVADA EN EL MÓDULO CRIPTOGRÁFICO

La clave privada de la EC debe crearse en el propio dispositivo. La recuperación de la clave privada en el módulo criptográfico debe realizarse al menos con el concurso de dos operadores autorizados.

28.3.6 MÉTODO DE ACTIVACIÓN DE LA CLAVE PRIVADA

La clave privada de la EC deberá ser activada conforme al apartado 29.3.1.

Se deberá proteger el acceso a la clave privada del Suscriptor por medio de una contraseña, PIN, u otros métodos de activación equivalentes. Si estos datos de activación deben ser entregados al Suscriptor, esta entrega deberá realizarse por medio de un canal seguro.

Estos datos de activación deberán tener una longitud de al menos 4 dígitos en el caso de custodia en un dispositivo hardware y de 8 en el caso de dispositivo software.

Los datos de activación deben ser memorizados por el Suscriptor y no deben ser anotados en un lugar de fácil acceso ni compartidos.

28.3.7 MÉTODO DE DESACTIVACIÓN DE LA CLAVE PRIVADA

La clave privada de la EC quedará desactivada mediante el borrado del contenido del dispositivo criptográfico que la contiene siguiendo estrictamente los manuales de administrador de dicho dispositivo.

La clave privada del suscriptor/titular quedará inaccesible después de sucesivos intentos en la introducción del código de activación.

28.3.8 MÉTODO PARA DESTRUIR LA CLAVE PRIVADA

La EC deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que la clave privada de la EC no será usada una vez finalizado su ciclo de vida.

Todas las copias de la clave privada de firma de la EC deberán ser destruidas o deshabilitadas de forma que la clave privada no pueda ser recuperada.

La destrucción o deshabilitación de las claves se detallará en un documento creado al efecto.

Las claves privadas de los Suscriptores deberán ser destruidas o hacerlas inservibles después del fin de su ciclo de vida por el propio Suscriptor.

28.4 OTROS ASPECTOS DE LA GESTIÓN DEL PAR DE CLAVES

28.4.1 ARCHIVO DE LA CLAVE PÚBLICA

La EC deberá conservar todas las claves públicas de verificación.

28.4.2 PERIODO DE USO PARA EL PAR DE CLAVES

Ya visto.

28.4.3 FINALIZACIÓN DE LA SUSCRIPCIÓN

La EC describe los procedimientos que pueden ser utilizados por el suscriptor para terminar la suscripción a los servicios de la EC, incluyendo: La revocación de los certificados al final de la suscripción (que pueden ser diferentes, dependiendo de si el final de la suscripción se debió a la expiración del certificado o resolución del servicio). La finalización de la suscripción puede darse cuando un suscriptor elija finalizar su suscripción como parte de la IOFE o la EC termine su suscripción al mismo, por fallecimiento del suscriptor o

extinción de la persona jurídica que es titular del certificado. Los procedimientos relativos a la Entidad de Certificación son descritos en el documento de Declaración y Política de Registro de LLAMA.PE.

28.5 DATOS DE ACTIVACIÓN

28.5.1 GENERACIÓN E INSTALACIÓN DE LOS DATOS DE ACTIVACIÓN

Los datos de activación de las EC se generan y se almacenan en smart cards criptográficas únicamente en posesión de personal autorizado.

28.5.2 PROTECCIÓN DE LOS DATOS DE ACTIVACIÓN

Solo el personal autorizado conoce los PINs y contraseñas para acceder a los datos de activación.

28.5.3 OTROS ASPECTOS DE LOS DATOS DE ACTIVACIÓN

No estipulados.

28.6 GESTIÓN DEL CICLO DE VIDA DEL MÓDULO CRIPTOGRÁFICO

Llama.pe debe proteger el módulo criptográfico donde se almacena la clave privada, a fin de evitar su compromiso.

- El módulo criptográfico no sera manipulado durante su transporte, ese sea hacia el centro de datos, su importación, o algún otro sitio autorizado por el responsable de la EC; para lo cual se mantendrá en su caja y sellada con cinta adhesiva de seguridad "VOID/OPEN" de transferencia total
- El módulo criptográfico no será manipulado durante su almacenamiento, con excepción del equipo designado para ponerlo en su rack en el centro de datos con supervisión del responsable de la EC, CISO o un miembro del Comité de Seguridad de Llama.pe asignado por el responsable de la EC.
- Procedimientos y controles deben proteger para restringir el acceso físico a sólo personal autorizado (A11-POL-006 POLÍTICA DE SEGURIDAD FÍSICA Y DEL ENTORNO)
- La instalación y activación de la clave de firma de Llama.pe EC en el módulo criptográfico será realizada sólo por personal que ocupa roles de confianza (Titulares de las claves), usando al menos un control de acceso de dos personas.
- Por medio enlaces web como el Nagios, Llama.pe EC verifica que el módulo criptográfico funcione correctamente
- Las claves de firma de la EC que son almacenadas en un módulo criptográfico deben ser borradas antes de que el dispositivo sea retirado.

28.7 CONTROLES DE SEGURIDAD INFORMÁTICA

LLAMA.PE emplea sistemas fiables para ofrecer sus servicios de certificación. LLAMA.PE ha realizado controles y auditorías informáticas a fin de establecer una gestión de sus activos informáticos adecuados con el nivel de seguridad requerido en la gestión de sistemas de certificación electrónica.

Respecto a la seguridad de la información se sigue el esquema de certificación sobre sistemas de gestión de la información ISO 270001.

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

1. Configuración de seguridad del sistema operativo.
2. Configuración de seguridad de las aplicaciones.
3. Dimensionamiento y planificación de demanda del sistema.
4. Configuración de Usuarios y permisos.
5. Configuración de eventos de registros de auditoría.
6. Plan de copia de respaldo y recuperación.
7. Configuración antivirus
8. Requerimientos de tráfico de red.

28.7.1 REQUISITOS TÉCNICOS DE SEGURIDAD ESPECÍFICOS

Cada servidor de LLAMA.PE incluye las siguientes funcionalidades:

- Control de acceso a los servicios de EC y gestión de privilegios.
- Imposición de separación de tareas para la gestión de privilegios.
- Identificación y autenticación de roles asociados a identidades.
- Archivo del historial del Firmante y la EC y datos de auditoría.
- Auditoría de eventos relativos a la seguridad.
- Auto-diagnóstico de seguridad relacionado con los servicios de la EC.
- Mecanismos de recuperación de claves y del sistema de EC Las funcionalidades expuestas son realizadas mediante una combinación de sistema operativo, software de PKI, protección física y procedimientos.

28.7.2 EVALUACIÓN DE LA SEGURIDAD INFORMÁTICA

La seguridad de los equipos viene reflejada por un análisis de riesgos iniciales de tal forma que las medidas de seguridad implantadas son respuesta a la probabilidad e impacto producido cuando un grupo de amenazas definidas puedan aprovechar brechas de seguridad.

28.8 CONTROLES TÉCNICOS DEL CICLO DE VIDA

28.8.1 CONTROLES DE DESARROLLO DE SISTEMAS

LLAMA.PE posee un procedimiento de control de cambios en las versiones de sistemas operativos y aplicaciones que impliquen una mejora en sus funciones de seguridad o que corrijan cualquier vulnerabilidad detectada. Como respuesta a los análisis de intrusión y vulnerabilidades se realizan las adaptaciones de los sistemas y aplicaciones que pueden tener problemas de seguridad y a las alertas de seguridad recibidas desde los servicios de seguridad gestionadas contratados con terceros, se realizan ejecutan los RFC (Request for Changes) correspondientes para la incorporación de los parches de seguridad o la actualización de las versiones con problemas.

En el RFC se incorporan y se documentan las medidas tomadas para la aceptación, ejecución o la denegación de dicho cambio. En los casos que la ejecución de la actualización o corrección de un problema incorpore una situación de vulnerabilidad o un riesgo importante se incorpora en el análisis de riesgos y se ejecutan controles alternativos hasta que el nivel de riesgo sea asumible.

28.8.2 CONTROLES DE GESTIÓN DE SEGURIDAD

LLAMA.PE desarrolla las actividades precisas para la formación y concienciación de los empleados en materia de seguridad. Los materiales empleados para la formación y los documentos descriptivos de los procesos son actualizados después de su aprobación por un grupo para la gestión de la seguridad. Para realizar esta función dispone de un plan de formación anual.

LLAMA.PE exige mediante contrato, las medidas de seguridad equivalentes a cualquier proveedor externo implicado en las labores de certificación.

28.8.3 CONTROLES DE SEGURIDAD DEL CICLO DE VIDA

Para proteger la gestión del ciclo de vida de las claves de la EC, Llama.pe cuenta con roles de confianza que se mencionan en la Política de Seguridad (punto 6.2.1)

28.9 CONTROLES DE SEGURIDAD DE LA RED

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

La información que se transfiere por redes no seguras se realiza de forma cifrada mediante uso de protocolos SSL.

28.10 SELLADO DE TIEMPO

Los sellos de tiempo de LLAMA.PE cumplen con lo siguiente:

- Los sellos de tiempo son conformes a la RFC 3161.
- Se utiliza un servicio de sincronización a una fuente de tiempo confiable.
- El sello de tiempo incluye un identificador de la política de sello de tiempo, en concordancia con la TSA y la TSU de LLAMA.PE.
- Cada sello de tiempo tiene asignado un único identificador.
- El valor de tiempo es trazable a la fuente de tiempo confiable del **INACAL**, la cual es reconocida por el Bureau International des Poids et Mesures (BIPM).
- El tiempo incluido en el sello de tiempo se encuentra sincronizado con la UTC dentro de la exactitud de +/-1 segundo.
- El sello de tiempo incluye un resumen de los datos firmados (HASH).
- El sello de tiempo se encuentra firmado por una clave generada para este propósito, correspondiente a la TSA de LLAMA.PE.
- Si se detecta que el reloj del sello de tiempo se encuentra fuera de la precisión indicada, los sellos de tiempo no se emitirán. Asimismo, los terceros que confían afectados serán informados al respecto.
- La sincronización del reloj se mantiene aun cuando se presenten cambios en el tiempo notificado por una
- Autoridad Competente. El cambio se realiza cuando el cambio en el tiempo se encuentra debidamente planificado.

Los procedimientos relativos a este punto son descritos en el documento Política de Seguridad de LLAMA.PE.

29 PERFILES DE CERTIFICADOS Y CRL

29.1 PERFIL DE CERTIFICADO

Todos los certificados emitidos bajo la Política de Certificación de Llama.pe serán conformes al estándar X.509 versión 3 y al RFC 3039 "Internet X.509 Public Key Infrastructure Qualified Certificates Profile".

29.1.1 NÚMERO DE VERSIÓN

LLAMA.PE emite certificados X.509 Versión 3.

29.1.2 EXTENSIONES DEL CERTIFICADO

El perfil del certificado está redactado en un documento independiente. Dicho documento debe estar a disposición de cualquier tercero que lo solicite.

29.1.3 EXTENSIÓN CON LAS FACULTADES DE REPRESENTACIÓN ESPECIAL

El certificado, emitido bajo la Política de Certificación de Llama.pe, incluirá una extensión en la que el solicitante detallará las facultades que le han sido otorgadas mediante poder notarial especial para la realización de determinados trámites en nombre y representación de la entidad.

29.1.4 EXTENSIONES ESPECÍFICAS

El certificado, emitido bajo la presente Política, podrá incluir por petición del suscriptor extensiones adicionales con información específica de su propiedad. Esta información estará bajo la exclusiva responsabilidad del suscriptor. Dichas extensiones no se marcarán como críticas y sean reconocibles como tales.

29.1.5 IDENTIFICADORES DE OBJETOS DE ALGORITMO

El identificador de objeto del algoritmo de firma será 1.2.840.113549.1.1.5

El identificador de objeto del algoritmo de la clave pública será rsa Encryption 1.2.840.113549.1.1.1

29.1.6 FORMATO DE NOMBRES

Los certificados deberán contener las informaciones que resulten necesarias para su uso, según determine la correspondiente política de autenticación, firma electrónica, cifrado o evidencia electrónica.

En general, los certificados de uso en el sector público deberán contener la identidad de la persona que los recibe, preferiblemente en los campos Subject Name o Subject Alternative Name, incluyendo los siguientes datos:

- Nombre y apellidos del Suscriptor, poseedor o representado, en campos separados, o con indicación del algoritmo que permite la separación de forma automática.
- Denominación social de la persona jurídica, cuando corresponda.
- Números de documentos de identificación correspondientes, de acuerdo con la legislación aplicable al Suscriptor, poseedor o representado, sea persona natural o jurídica.

Esta norma no se aplica a los certificados con seudónimo, que deben identificar esta condición. La semántica exacta de los nombres se describe en las fichas de los perfiles.

29.1.7 LIMITACIONES DE LOS NOMBRES

Se puede utilizar restricciones de nombre (utilizando la extensión del certificado "name constrains") en aquellos certificados de la EC de LLAMA.PE emitidos a terceras partes de forma que solo se pueda emitir por la EC el conjunto de certificados permitido en dicha extensión.

29.2 PERFIL DE CRL

El perfil del certificado de CRL está redactado en un documento independiente. Dicho documento debe estar a disposición de cualquier tercero que lo solicite.

29.2.1 NÚMERO DE VERSIÓN

El formato de las CRLs utilizadas es el especificado en la versión 2 (X.509 v2).

29.2.2 CRL Y EXTENSIONES CRL

Se soporta y se utilizan CRLs conformes al estándar X.509.

29.3 PERFIL DE OCSP

El perfil OCSP está redactado en un documento independiente. Dicho documento debe estar a disposición de cualquier tercero que lo solicite.

30 AUDITORÍA DE CONFORMIDAD Y OTROS CONTROLES

LLAMA.PE se somete a auditorías periódicas como se describe en los apartados siguientes.

30.1 FRECUENCIA O CIRCUNSTANCIAS DE LOS CONTROLES

LLAMA.PE lleva a cabo auditorías internas y externas. La auditoría interna se llevará a cabo una vez al año. Así mismo, las evaluaciones técnicas del INDECOPI se llevarán a cabo una vez al año y/o cada vez que el INDECOPI lo requiera.

30.2 IDENTIDAD/CALIFICACIÓN DEL AUDITOR

INDECOPI se encarga de enviar un listado de auditores siendo decisión de la EC de LLAMA.PE la selección del auditor de dicha lista.

30.3 RELACIÓN ENTRE EL AUDITOR Y LA ENTIDAD AUDITADA

Los auditores son independientes de la EC de LLAMA.PE.

30.4 ASPECTOS CUBIERTOS POR LOS CONTROLES

En líneas generales, las auditorías verifican:

1. Que la EC tiene un sistema que garantiza la calidad del servicio prestado.
2. Que la EC cumple con los requerimientos de las Políticas de Certificación que gobiernan la emisión de los distintos certificados digitales.
3. Que la CPS, se ajusta a lo establecido en las Políticas, con lo acordado por la AAC y con lo establecido en la normativa vigente.
4. Que la EC gestione de forma adecuada la seguridad de sus sistemas de información.

30.5 TRATAMIENTOS DE LOS INFORMES DE AUDITORÍA

Una vez recibido el informe de la auditoría llevada a cabo, LLAMA.PE tomará las acciones correspondientes. LLAMA.PE ha desarrollado un documento Plan de auditorías que detalla este tipo de evaluación.

31 OTROS ASUNTOS LEGALES Y COMERCIALES

31.1 TARIFAS

31.1.1 TARIFAS DE EMISIÓN DE CERTIFICADOS Y RENOVACIÓN

Los precios de los servicios de certificación o cualquiera otros servicios relacionados estarán disponibles en la página web de LLAMA.PE.

31.1.2 TARIFAS DE ACCESO A LOS CERTIFICADOS

El acceso a los certificados emitidos es gratuito, no obstante, la EC se reserva el derecho de imponer alguna tarifa para los casos de descarga masiva de CRLs o cualquier otra circunstancia que a juicio de la EC deba ser gravada.

31.1.3 TARIFAS DE ACCESO A LA INFORMACIÓN RELATIVA AL ESTADO DE LOS CERTIFICADOS O LOS CERTIFICADOS REVOCADOS

La EC proveerá de un acceso a la información relativa al estado de los certificados libre y gratuita.

31.1.4 TARIFAS POR EL ACCESO AL CONTENIDO DE ESTAS POLÍTICAS DE CERTIFICACIÓN

El acceso al contenido de la presente Política de Certificación será gratuito.

31.1.5 POLÍTICA DE REINTEGROS

La EC dispondrá de una política de reintegros que se encuentra descrita en los contratos con los suscriptores.

31.2 RESPONSABILIDAD DE LLAMA.PE CA

La EC dispondrá en todo momento de una póliza de seguro en los términos que marque la legislación vigente. La EC actuará en la cobertura de sus responsabilidades por sí o a través de la entidad aseguradora, satisfaciendo los requerimientos de los solicitantes de los

certificados, de los Suscriptores y de los terceros que confíen en los certificados.

La EC será responsable del daño causado ante el Suscriptor o cualquier persona que de buena fe confíe en el certificado, siempre que exista dolo o culpa grave, respecto de:

1. La exactitud de toda la información contenida en el certificado en la fecha de su emisión
2. La garantía de que, en el momento de la entrega del certificado, obra en poder del Suscriptor o servicio electrónico, la clave privada correspondiente a la clave pública dada o identificada en el certificado
3. La garantía de que la clave pública y privada funcionan conjunta y complementariamente
4. La correspondencia entre el certificado solicitado y el certificado entregado
5. Cualquier responsabilidad que se establezca por la legislación vigente.

31.2.1 EXONERACIÓN DE RESPONSABILIDAD

La EC y ER de LLAMA.PE no serán responsables en ningún caso cuando se encuentran ante cualquiera de estas circunstancias:

1. Estado de Guerra, desastres naturales o cualquier otro caso de Fuerza Mayor
2. Por el uso de los certificados siempre y cuando exceda de lo dispuesto en la normativa vigente y la presente Política de Certificación
3. Por el uso indebido o fraudulento de los certificados o CRL's emitidos por la Autoridad de Certificación
4. Por el uso de la información contenida en el Certificado o en la CRL.
5. Por el incumplimiento de las obligaciones establecidas para el Suscriptor o Terceros que confían en la normativa vigente, la presente CPS o en las Prácticas Correspondientes.
6. Por el perjuicio causado en el periodo de verificación de las causas de revocación /suspensión.
7. Por el contenido de los mensajes o documentos firmados o cifrados digitalmente.
8. Por la no recuperación de documentos cifrados con la clave pública del Suscriptor.
9. Fraude en la documentación presentada por el solicitante.

31.3 RESPONSABILIDADES FINANCIERAS

La EC de LLAMA.PE dispone de una póliza de seguro que contempla sus responsabilidades, para indemnizar por daños y perjuicios que se puedan ocasionar a los usuarios de sus servicios, por un monto que supera lo establecido por la normativa vigente. La EC otorga al cliente una garantía de devolución de dinero dentro de los 7 (siete) días calendario de haber realizado el pago y no se haya descargado el certificado (incluye sábados, domingos y feriados) cuando la omisión o error es atribuible a la EC.

Excepciones de garantía: La EC se exceptúa de brindar la garantía del servicio cuando se evidencia que la omisión o error no es atribuible a la EC. INDEMNIZACIONES: La EC indemniza por el servicio de acuerdo al monto establecido en la normativa vigente.

31.4 CONFIDENCIALIDAD DE LA INFORMACIÓN COMERCIAL

31.4.1 TIPO DE INFORMACIÓN A MANTENER CONFIDENCIAL

Se considerará confidencial toda la información que no esté catalogada expresamente como pública. No se difunde información declarada como confidencial sin el consentimiento expreso por escrito de la entidad u organización que la haya otorgado el carácter confidencial a dicha información, a no ser que exista una imposición legal.

LLAMA.PE, dispone de una adecuada política de tratamiento de la información y de los modelos de acuerdo de confidencialidad que deberán firmar todas las personas que tengan acceso a información confidencial.

Asimismo, cumple en todo caso con la normativa vigente en cada momento en materia de protección de datos. En este sentido, este documento sirve, de conformidad con la Ley de Protección de Datos Personales – Ley N°29733, la Norma Marco de Privacidad y la Guía de Acreditación para Entidades de Certificación Digital y Entidades Conexas, en los ámbitos legales, regulatorios y contractuales.

31.4.2 TIPO DE INFORMACIÓN CONSIDERADA NO CONFIDENCIAL

Se considera como información no confidencial:

- La contenida en la presente CPS y en las Políticas.
- La información contenida en los certificados.
- Cualquier información cuya accesibilidad sea prohibida por la normativa vigente.

31.5 DERECHOS DE PROPIEDAD INTELECTUAL

La EC de LLAMA.PE es titular de los derechos de propiedad intelectual, que puedan derivarse del sistema de certificación que regula esta CPS y sus políticas. Se prohíbe por tanto, cualquier acto de reproducción, distribución, comunicación pública y transformación de cualquiera de los elementos que son titularidad exclusiva de la EC sin la autorización expresa por su parte.

No obstante, no necesitará autorización de la EC para la reproducción del Certificado cuando la misma sea necesaria para su utilización por parte del Tercero que confía legítimo y con arreglo a la finalidad del Certificado, de acuerdo con los términos de esta CPS y sus Políticas.

31.6 OBLIGACIONES

31.6.1 ENTIDAD DE CERTIFICACIÓN LLAMA.PE

LLAMA.PE se encuentra obligada a cumplir con lo dispuesto por la normativa vigente y además a:

1. Respetar lo dispuesto en esta Política.
2. Proteger sus claves privadas de forma segura.
3. Emitir certificados conforme a esta Política y a los estándares de aplicación.
4. Emitir certificados según la información que obra en su poder y libres de errores de entrada de datos
5. Emitir certificados cuyo contenido mínimo sea el definido por la normativa vigente para los certificados cualificados.
6. Publicar los certificados emitidos en un directorio, respetando en todo caso lo dispuesto en materia de protección de datos por la normativa vigente.
7. Suspender y revocar los certificados según lo dispuesto en esta Política y publicar las mencionadas revocaciones en la CRL
8. Informar a los Suscriptores de la revocación o suspensión de sus certificados, en tiempo y forma de acuerdo con la legislación vigente.
9. Publicar esta Política y las Prácticas correspondientes en su página web.
10. Informar sobre las modificaciones de la Política y Declaración Prácticas de Certificación de LLAMA.PE, a los Suscriptores y a la ER vinculada.
11. No almacenar ni copiar los datos de creación de firma del Suscriptor.
12. Proteger, con el debido cuidado, los datos de creación de firma mientras estén bajo su custodia, en su caso.
13. Establecer los mecanismos de generación y custodia de la información relevante en las actividades descritas, protegiéndolas ante pérdida o destrucción o falsificación
14. Conservar la información sobre el certificado emitido por el período mínimo exigido por la normativa vigente.

31.6.2 ENTIDAD DE REGISTRO LLAMA.PE

La ER de LLAMA.PE se encuentra obligada a cumplir con lo dispuesto por la normativa vigente y además a:

1. Respetar lo dispuesto en esta Política.
2. Proteger sus claves privadas.
3. Comprobar la identidad de los solicitantes de certificados
4. Verificar la exactitud y autenticidad de la información suministrada por el Suscriptor solicitante.
5. Archivar, por periodo dispuesto en la legislación vigente, los documentos suministrados por el Suscriptor.
6. Respetar lo dispuesto en los contratos firmados con la EC de LLAMA.PE y con el Suscriptor
7. Informar a la EC las causas de revocación, siempre y cuando tomen conocimiento.

31.6.3 ENTIDADES DE REGISTRO ANEXAS A LA EC DE LLAMA.PE

Las ER anexas se encuentran obligadas a cumplir con los dispuestos por la normativa vigente y además a:

1. Proteger sus claves privadas

2. Comprobar la identidad de los solicitantes de certificados
3. Verificar con exactitud y autenticidad la información suministrada por el Suscriptor solicitante
4. Archivar, por periodo dispuesto en la legislación vigente, los documentos suministrados por el Suscriptor
5. Pasar por una auditoria de parte de Llama.pe EC una vez al año
6. Respetar los dispuesto en los contratos firmados con la EC de Llama.pe y con el suscriptor
7. Informar a la EC las causas de revocación siempre y cuando tomen conocimiento
8. El Administrador y el Responsable de la ER anexa son los que gestionan el IP de su personal con el fin de que puedan acceder a la plataforma de certificados. Además del certificado digital de cada operador que ingresa a la plataforma, es necesario que se habilite su IP para que puedan acceder.

Para la verificación de antecedentes de los operadores de registro de las entidades de registro anexas a la EC se solicitarán los siguientes documentos:

- Antecedentes crediticios

- Antecedentes penales y policiales

- Documentación (solicitud de alta)

- Constancia de capacitación como Operador de Registro

- Constancia de aprobación del examen de OR otorgado por la EC de Llama.pe

31.6.4 SOLICITANTE

El solicitante de un Certificado estará obligado a cumplir con lo dispuesto por la normativa aplicable y además a:

1. Suministrar a la ER la información necesaria para realizar una correcta identificación.
2. Confirmar la exactitud y veracidad de la información suministrada.
3. Notificar cualquier cambio en los datos aportados para la creación del certificado durante su periodo de validez.

31.6.5 SUSCRIPTOR

El Suscriptor (ya sea persona natural o jurídica a través de un representante suficiente) de un certificado estará obligado a cumplir con lo dispuesto por la normativa vigente y además a:

1. Custodiar su clave privada de manera diligente
2. Usar el certificado según lo establecido en la presente Política de Certificación
3. Respetar lo dispuesto en el contrato firmado con la EC de LLAMA.PE.
4. En el caso de los certificados con alguna vinculación empresarial, informar de la existencia de alguna causa de suspensión /revocación como, por ejemplo, el cese o la modificación de su vinculación con la Entidad.
5. En el caso de los certificados con alguna vinculación empresarial, notificar cualquier cambio en los datos aportados para la creación del certificado durante su período de validez, como el cese o la modificación de su vinculación con la Entidad.

31.6.6 TERCERO QUE CONFÍA

Será obligación de los Terceros que confían cumplir con lo dispuesto por la normativa vigente y además:

1. Verificar la validez de los certificados en el momento de realizar cualquier operación basada en los mismos.
2. Conocer y sujetarse a las garantías, límites y responsabilidades aplicables en la aceptación y uso de los certificados en los que confía, y aceptar sujetarse a las mismas.

31.6.7 EMPRESAS

En el caso de que el certificado exprese alguna vinculación empresarial será obligación de la Empresa solicitar a la ER la suspensión/revocación del certificado cuando cese o se modifique la vinculación del Suscriptor o el servicio electrónico con la Empresa.

31.6.8 REPOSITORIO

La información relativa a la publicación y revocación /suspensión de los certificados se mantendrá accesible al público en los términos establecidos en la normativa vigente. La EC deberá mantener un sistema seguro de almacén y recuperación de certificados y un repositorio de certificados revocados, pudiendo delegar estas funciones en una tercera entidad.

32 RESOLUCIÓN DE DISPUTAS

Para la resolución de disputas el titular/suscriptor escribe desde el correo electrónico que brindó a la ER con los argumentos de la disputa en mención al correo electrónico de la ENTIDAD soporte@llama.pe para su revisión y del ser del ámbito será atendido brindando respuesta al titular/suscriptor.
De llegar a alguna disputa o incumplimiento entre las partes, los costos incluido el honorario de abogados será asumida por cada parte.

33 CONFORMIDAD CON LA LEY APLICABLE

LLAMA.PE es afecta y cumple con las obligaciones establecidas por la IOFE, a los requerimientos de la Guía de Acreditación para Entidades de Certificación Digital EC, al Reglamento de la Ley de Certificados Digitales, y a la Ley de Firmas y Certificados Digitales – Ley 27269, para el reconocimiento legal de los servicios que brinda la EC de LLAMA.PE bajo las directrices definidas en el presente documento.

34 BIBLIOGRAFÍA

1. Guía de Acreditación para Entidades de Certificación Digital EC, INDECOPI
2. Ley de Firmas y Certificados Digitales – Ley 27269
3. Decreto Supremo 052-2008
4. Decreto Supremo 070-2011
5. Decreto Supremo 105-2012