llama.pe

# POLÍTICA DE CERTIFICACIÓN

VERSIÓN: V1.7

PUBLICO

OFICIAL

PARA: LLAMA.PE

HISTORIAL DE VERSIONES

| VERSIÓN | DESCRIPCIÓN | REALIZADO POR | FECHA |
|---|---|---|---|
| V1.7 | 1.7 05/06/2023 Correcciones de espaciado, gramática y puntuación. Se agregan los puntos "20.1.1, 20.1.2 y 20.1.3" para explicar el procedimiento de emisión de certificados. | JORGE ENRIQUE MIGUEL ZELAYARÁN SANCHEZ | 2023-06-06 |
| V1.6 | 1.0 25/06/2018 25/06/2018 Elaboración de documento inicial. 1.1 19/07/2018 19/07/2018 Se induye el OID de la política y los tipos de soporte de cada certificado. 1.2 22/08/2018 22/08/2018 Se modifica la estructura del documento. 1.3 8/8/2019 08/08/2019 Se modifica conceptos y actualización para brindar el servicio a nuevas ER 1.4 19/02/2020 19/02/2020 Se agrega perfil de certificado TSU en la sección 6.3 1.5 10/03/2021 10/03/2021 actualización de formato 1.6 17/09/2022 Actualización en el punto 8.1 | LOUIE ALBERTO DIAZ MARTICORENA | 2022-12-27 |

# Tabla de contenido


- 1 INTRODUCCIÓN
- 2 OBJETIVO
- 3 OBJETO DE LA ACREDITACIÓN
- 4 DEFINICIONES Y ABREVIACIONES
  - 4.1 ABREVIACIONES
  - 4.2 DEFINICIONES
- 5 PKI PARTICIPANTES
  - 5.1 ENTIDAD DE CERTIFICACIÓN LLAMA.PE (EC LLAMA.PE)
  - 5.2 ENTIDAD DE REGISTRO LLAMA.PE (ER LLAMA.PE)
  - 5.3 TITULAR
  - 5.4 SUSCRIPTOR
  - 5.5 SOLICITANTE
  - 5.6 TERCERO QUE CONFÍA
  - 5.7 OTROS PARTICIPANTES
- 6 PKI LLAMA.PE
  - 6.1 GENERALIDADES
  - 6.2 IDENTIFICACIÓN
  - 6.3 POLÍTICAS DE CERTIFICACIÓN
  - 6.4 TIPOS DE SOPORTE
    - 6.4.1 SOFTWARE
    - 6.4.2 DSCF
- 7 RESPONSABILIDADES
- 8 ÁMBITO DE APLICACIÓN Y USOS
  - 8.1 TIPOS DE CERTIFICADO
  - 8.2 USOS ADECUADOS DEL CERTIFICADO
  - 8.3 USOS PROHIBIDOS DEL CERTIFICADO
- 9 PERSONA DE CONTACTO
- 10 CLÁUSULAS GENERALES
  - 10.1 OBLIGACIONES
    - 10.1.1 ENTIDAD DE CERTIFICACIÓN LLAMA.PE
    - 10.1.2 ENTIDAD DE REGISTRO LLAMA.PE
    - 10.1.3 SOLICITANTE
    - 10.1.4 SUSCRIPTOR
    - 10.1.5 TERCERO QUE CONFÍA
    - 10.1.6 EMPRESAS
    - 10.1.7 REPOSITORIO
  - 10.2 RESPONSABILIDAD
    - 10.2.1 EXONERACIÓN DE RESPONSABILIDAD
    - 10.2.2 LÍMITE DE RESPONSABILIDAD EN CASO DE PÉRDIDAS POR TRANSACCIONES
  - 10.3 RESPONSABILIDAD FINANCIERA
  - 10.4 TARIFAS
    - 10.4.1 TARIFAS DE EMISIÓN DE CERTIFICADOS Y RENOVACIÓN

        - 10.4.2 TARIFAS DE ACCESO A LOS CERTIFICADOS
        - 10.4.3 TARIFAS DE ACCESO A LA INFORMACIÓN RELATIVA AL ESTADO DE LOS CERTIFICADOS O LOS CERTIFICADOS REVOCADOS
        - 10.4.4 TARIFAS POR EL ACCESO AL CONTENIDO DE ESTAS POLÍTICAS DE CERTIFICACIÓN
        - 10.4.5 POLÍTICA DE REINTEGROS
- 11 ORGANIZACIÓN QUE ADMINISTRA LOS DOCUMENTOS DE CP y CPS
- 12 PUBLICACIÓN DE LA DECLARACIÓN DE PRÁCTICAS
- 13 RESPONSABILIDADES SOBRE REPOSITORIOS Y PUBLICACIÓN DE INFORMACIÓN
    - 13.1 PUBLICACIÓN DE LA INFORMACIÓN DE CERTIFICACIÓN
    - 13.2 PLAZO O FRECUENCIA DE LA PUBLICACIÓN
    - 13.3 CONTROLES DE ACCESO A LOS REPOSITORIOS
- 14 IDENTIFICACION Y AUTENTICACION
    - 14.1 NOMBRES
        - 14.1.1 TIPOS DE NOMBRES
        - 14.1.2 NECESIDAD DE QUE LOS NOMBRES TENGAN SIGNIFICADO
        - 14.1.3 ANONIMATO Y PSEUDO ANONIMATO DE LOS TITULARES
        - 14.1.4 REGLAS PARA LA INTERPRETACIÓN DE VARIAS FORMAS DE NOMBRE
        - 14.1.5 SINGULARIDAD DE LOS NOMBRES
        - 14.1.6 RECONOCIMIENTO, AUTENTICACIÓN Y PAPEL DE LAS MARCAS RECONOCIDAS.
- 15 VALIDACIÓN INICIAL DE LA IDENTIDAD
    - 15.1 MÉTODO PARA DEMOSTRAR LA POSESIÓN DE LA CLAVE PRIVADA
    - 15.2 AUTENTICACIÓN DE LA IDENTIDAD DE UNA ORGANIZACIÓN (PERSONA JURÍDICA)
    - 15.3 AUTENTICACIÓN DE UNA IDENTIDAD INDIVIDUAL (PERSONA NATURAL)
    - 15.4 INFORMACIÓN DE TITULAR NO VERIFICADA
    - 15.5 VALIDACIÓN DE LA AUTORIDAD
    - 15.6 CRITERIOS PARA LA INTEROPERABILIDAD
- 16 IDENTIFICACIÓN Y AUTENTICACIÓN PARA PETICIONES DE RE-EMISIÓN DE CLAVES
    - 16.1 IDENTIFICACIÓN Y AUTENTICACIÓN PARA RE-EMISIÓN DE RUTINA
    - 16.2 IDENTIFICACIÓN Y AUTENTICACIÓN TRAS UNA REVOCACIÓN
- 17 IDENTIFICACIÓN Y AUTENTICACIÓN PARA PETICIONES DE REVOCACIÓN
- 18 REQUISITOS OPERACIONALES PARA EL CICLO DE VIDA DE LOS CERTIFICADOS
    - 18.1 SOLICITUD DEL CERTIFICADO
    - 18.2 QUIÉN PUEDE SOLICITAR UN CERTIFICADO
    - 18.3 PROCESO DE REGISTRO Y RESPONSABILIDADES
- 19 TRAMITACIÓN DE SOLICITUD DE CERTIFICADOS
    - 19.1 REALIZACIÓN DE LAS FUNCIONES DE IDENTIFICACIÓN Y AUTENTICACIÓN
    - 19.2 APROBACIÓN O RECHAZO DE LAS SOLICITUDES DE CERTIFICADO
    - 19.3 PLAZO PARA PROCESAR LAS SOLICITUDES DE CERTIFICADO
- 20 EMISIÓN DE CERTIFICADOS
    - 20.1 ACTUACIONES DE LA EC DURANTE LA EMISIÓN DE CERTIFICADOS
        - 20.1.1 EMISIÓN DE CERTIFICADO MEDIANTE SOFTWARE (.pfx o .p12)
        - 20.1.2 EMISIÓN DE CERTIFICADO MEDIANTE HARDWARE
        - 20.1.3 EMISIÓN DE CERTIFICADO MEDIANTE WATANA APP
    - 20.2 NOTIFICACIÓN AL SUSCRIPTOR POR LA EC DE LA EMISIÓN DEL CERTIFICADO
- 21 ACEPTACIÓN DEL CERTIFICADO
    - 21.1 FORMA EN LA QUE SE ACEPTA EL CERTIFICADO
    - 21.2 PUBLICACIÓN DEL CERTIFICADO POR LA EC
    - 21.3 NOTIFICACIÓN DE LA EMISIÓN DEL CERTIFICADO POR LA EC A OTRAS ENTIDADES
- 22 USO DE LA CLAVE PRIVADA Y DEL CERTIFICADO
    - 22.1 USO DE LA CLAVE PRIVADA Y DEL CERTIFICADO POR EL TITULAR/SUSCRIPTOR
    - 22.2 USO DE LA CLAVE PRIVADA Y DEL CERTIFICADO POR TERCEROS QUE CONFÍAN
- 23 RENOVACIÓN DEL CERTIFICADO SIN CAMBIO DE CLAVES
- 24 RE-EMISIÓN DEL CERTIFICADO CON CAMBIO DE CLAVES
    - 24.1 CIRCUNSTANCIAS PARA LA RE-EMISIÓN DE CERTIFICADOS CON CAMBIO DE CLAVES
    - 24.2 QUIÉN PUEDE SOLICITAR UNA RE-EMISIÓN CON CAMBIO DE CLAVES.
    - 24.3 TRÁMITES PARA LA SOLICITUD DE RE-EMISIÓN DE CERTIFICADOS CON CAMBIO DE CLAVES.
    - 24.4 NOTIFICACIÓN AL TITULAR DE LA EMISIÓN DE UN NUEVO CERTIFICADO CON CAMBIO DE CLAVES

    - 24.5 FORMA EN LA QUE SE ACEPTA LA RE-EMISIÓN DE UN CERTIFICADO
    - 24.6 PUBLICACIÓN DEL CERTIFICADO RE-EMITIDO POR LA EC
    - 24.7 NOTIFICACIÓN DE LA EMISIÓN DE UN CERTIFICADO RE-EMITIDO POR LA EC A OTRAS ENTIDADES
- 25 MODIFICACIÓN DE CERTIFICADOS
- 26 REVOCACIÓN Y SUSPENSIÓN DE CERTIFICADOS
    - 26.1 CIRCUNSTANCIAS PARA LA REVOCACIÓN DE UN CERTIFICADO
    - 26.2 QUIÉN PUEDE SOLICITAR UNA REVOCACIÓN
    - 26.3 PROCEDIMIENTO DE SOLICITUD DE REVOCACIÓN
    - 26.4 PERIODO DE GRACIA DE SOLICITUD DE REVOCACIÓN
    - 26.5 PLAZO EN EL QUE LA EC DEBE RESOLVER LA SOLICITUD DE REVOCACIÓN
    - 26.6 REQUISITOS DE VERIFICACIÓN DE LAS REVOCACIONES POR LOS TERCEROS QUE CONFÍAN
    - 26.7 FRECUENCIA DE EMISIÓN DE LAS CRLS
    - 26.8 TIEMPO MÁXIMO DE LATENCIA DE LAS CRLS
    - 26.9 DISPONIBILIDAD DE VERIFICACIÓN DEL ESTADO
    - 26.10 REQUISITOS DE COMPROBACIÓN DE LA REVOCACIÓN ON-LINE
    - 26.11 OTRAS FORMAS DISPONIBLES DE DIVULGACIÓN DE INFORMACIÓN DE REVOCACIÓN
    - 26.12 REQUISITOS ESPECIALES DE RENOVACIÓN DE CLAVES COMPROMETIDAS
    - 26.13 CIRCUNSTANCIAS PARA LA SUSPENSIÓN
- 27 SERVICIOS DE INFORMACIÓN DEL ESTADO DE CERTIFICADOS
    - 27.1 CARACTERÍSTICAS OPERACIONALES
    - 27.2 DISPONIBILIDAD DEL SERVICIO
- 28 FINALIZACIÓN DE SUSCRIPCIÓN
- 29 ALMACENAMIENTO Y RECUPERACIÓN DE LA CLAVE (CERTIFICADOS DE CIFRADO)
- 30 CONTROLES FÍSICOS DE LA INSTALACIÓN, GESTIÓN, COMPUTACIONALES Y OPERACIONALES
- 31 CONTROLES TÉCNICOS DE SEGURIDAD
- 32 CAMBIO DE CLAVES
- 33 AUDITORÍA DE CONFORMIDAD Y OTROS CONTROLES
- 34 COMPROMISO DEL RECUPERACION DE DESASTRES
- 35 FINALIZACIÓN DE EC
- 36 GENERACIÓN E INSTALACIÓN DEL PARA DE LLAVES
- 37 PROTECCIÓN DE LA CLAVE PRIVADA
- 38 DESTRUCCIÓN DE LAS CLAVES
- 39 DATOS DEL ACTIVACION
- 40 PERFILES DE CERTIFICADOS, OSCP Y CRL
    - 40.1 PERFIL DE CERTIFICADO
    - 40.2 NÚMERO DE VERSIÓN
        - 40.2.1 EXTENSIONES DEL CERTIFICADO
        - 40.2.2 EXTENSIÓN CON LAS FACULTADES DE REPRESENTACIÓN ESPECIAL
        - 40.2.3 EXTENSIONES ESPECÍFICAS
        - 40.2.4 FORMATO DE NOMBRES
        - 40.2.5 LIMITACIONES DE LOS NOMBRES
    - 40.3 PERFIL DE CRL
        - 40.3.1 NÚMERO DE VERSIÓN
        - 40.3.2 CRL Y EXTENSIONES CRL
    - 40.4 PERFIL DE OSCP
- 41 OTROS ASUNTOS LEGALES Y COMERCIALES
    - 41.1 CONFIDENCIALIDAD DE LA INFORMACIÓN COMERCIAL
        - 41.1.1 TIPO DE INFORMACIÓN A MANTENER CONFIDENCIAL
        - 41.1.2 TIPO DE INFORMACIÓN CONSIDERADA NO CONFIDENCIAL
    - 41.2 DERECHOS DE PROPIEDAD INTELECTUAL
    - 41.3 OBLIGACIONES
        - 41.3.1 ENTIDAD DE CERTIFICACIÓN LLAMA.PE
        - 41.3.2 ENTIDAD DE REGISTRO LLAMA.PE
        - 41.3.3 SOLICITANTE
        - 41.3.4 SUSCRIPTOR
        - 41.3.5 TERCERO QUE CONFÍA

        - 41.3.6 EMPRESAS
        - 41.3.7 REPOSITORIO
    - 41.4 VIGENCIA Y CONCLUSIÓN
    - 41.5 CONCLUSIONES Y ENMIENDAS
    - 41.6 RESOLUCIÓN DE DISPUTAS
- 42 CLÁUSULAS MISCELÁNEAS
    - 42.1 ACUERDO INTEGRO
    - 42.2 ASIGNACIÓN
    - 42.3 DIVISIBILIDAD
    - 42.4 EJECUCIÓN
    - 42.5 FUERZA MAYOR
- 43 CONFORMIDAD CON LA LEY APLICABLE
- 44 BIBLIOGRAFÍA

# POLÍTICA 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 servicios 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 cuanto a los tipos de certificados digitales reconocidos por INDECOPI, se encuentran: Certificados digitales de Representante legal, de Atributos y de Agente Automatizado.

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

# 2 OBJETIVO

Este documento tiene como objetivo la descripción de las prácticas, los perfiles y los tipos de usuarios y usos definidos para LLAMA.PE, de acuerdo a lo estipulado en la Política de Certificación, para la administración de los certificados digitales en el marco del cumplimiento de los requerimientos de la "Guía de Acreditación de Entidades de Certificación Digital (EC)" establecida por el INDECOPI.

# 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

## 4.2 DEFINICIONES

Entidad de Certificación – EC: Entidad que presta servicios de emisión, revocación, re-emisión, modificación, suspensión 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.

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.

# 5 PKI PARTICIPANTES

## 5.1 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.

## 5.2 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.

## 5.3 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.

## 5.4 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 de suscriptor recaerá sobre el representante legal designado por esta entidad. Si el certificado está designado para ser usado por un agente automatizado, la titularidad del certificado

y de las firmas digitales generadas a partir de dicho certificado corresponderá a la persona jurídica. La atribución de responsabilidad del suscriptor, para tales efectos, corresponde a la misma persona jurídica.

## 5.5 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.

## 5.6 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.

## 5.7 OTROS PARTICIPANTES

Se considera como otros participantes a proveedores que participan en el servicio de Certificación, como: Proveedores del servicio del repositorio, Data center, entre otros.

# 6 PKI LLAMA.PE

## 6.1 GENERALIDADES

LLAMA.PE ha establecido una Política de Certificación para los diferentes certificados emitidos por la PKI LLAMA.PE, la cual se encuentra basada en la especificación del estándar RCF 2527 – Internet X. 509 Public Key Infrastructure Certificate Policy.

## 6.2 IDENTIFICACIÓN

La PKI LLAMA.PE está identificada con el OID:

1.3.6.1.4.1. 52215.0

iso (1)

org (3)

dod (6)

internet (1)

private (4)

enterprise (1)

LLAMA.PE S.A (52215)

PKI LLAMA.PE (0)

## 6.3 POLÍTICAS DE CERTIFICACIÓN

LLAMA.PE cuenta con un OID para cada tipo certificado, tal y como se describe a continuación.

| NOMBRE | OID |
|---|---|

| | |
|---|---|
| Política de certificado de Persona Natural | 1.3.6.1.4.1. 52215.0.1.0.1.S |
| Política de certificado de Persona Jurídica | 1.3.6.1.4.1. 52215.0.1.0.2.S |
| Política de certificado de Agente Automatizado | 1.3.6.1.4.1. 52215.0.1.0.3.S |
| Política de certificado de TSU | 1.3.6.1.4.1. 52215.0.1.0.4.1 |

S = Tipo de Soporte

1 = Software

2 = DSCF (HSM, token , tarjeta criptográfica)

## 6.4 TIPOS DE SOPORTE

### 6.4.1 SOFTWARE

Los certificados de Persona Natural, Persona Jurídica y Agente Automatizado; pueden ser emitidos en formato software.

### 6.4.2 DSCF

Los certificados de Persona Natural, Persona Jurídica y Agente Automatizado; pueden ser emitidos en formato DSCF.

Solo los certificados de Persona Jurídica también pueden ser emitidos mediante un dispositivo seguro de creación de firma en el caso de Operadores de Registro de la EC de LLAMA.PE.

# 7 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.

# 8 ÁMBITO DE APLICACIÓN Y USOS

## 8.1 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.
- Certificado de persona jurídica: Es el tipo de certificado que identifica al Firmante como Representante legal o Apoderado de una Organización o Entidad.
- Certificado de persona jurídica de Atributos: Es el tipo de certificado que identifica al Firmante como colaborador, empleado, 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.
- 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.

## 8.2 USOS ADECUADOS DEL CERTIFICADO

Los Certificados emitidos bajo la 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 repudiar, es decir, el Titular que ha firmado no puede negar la autoría o la integridad del mismo.

## 8.3 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.

# 9 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/

# 10 CLÁUSULAS GENERALES

## 10.1 OBLIGACIONES

### 10.1.1 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.

### 10.1.2 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.

### 10.1.3 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.

### 10.1.4 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.

### 10.1.5 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.

### 10.1.6 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.

### 10.1.7 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.

## 10.2 RESPONSABILIDAD

La EC dispondrá en todo momento de un seguro de responsabilidad civil 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.

### 10.2.1 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 Política de Certificación 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

### 10.2.2 LÍMITE DE RESPONSABILIDAD EN CASO DE PÉRDIDAS POR TRANSACCIONES

La EC de LLAMA.PE no aplicará límites de cantidad a las transacciones que se realicen con el certificado. Podrán establecerse garantías particulares a través de seguros específicos que se negociarán individualmente. Esta garantía será de aplicación a efectos de lo dispuesto en legislación vigente.

## 10.3 RESPONSABILIDAD FINANCIERA

La EC de LLAMA.PE dispone de garantías bancarias para cumplir con sus responsabilidades, para indemnizar por daños y perjuicios que se puedan ocasionar a los usuarios de sus servicios.

GARANTÍAS: La EC otorga al cliente una garantía de devolución de dinero dentro de los 7 (siete) días calendarios después de descargar el Certificado Digital 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

## 10.4 TARIFAS

### 10.4.1 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.

### 10.4.2 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.

### 10.4.3 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.

### 10.4.4 TARIFAS POR EL ACCESO AL CONTENIDO DE ESTAS POLÍTICAS DE CERTIFICACIÓN

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

### 10.4.5 POLÍTICA DE REINTEGROS

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

# 11 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

# 12 PUBLICACIÓN DE LA DECLARACIÓN DE PRÁCTICAS

La Política de Certificación, 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/repository

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 ER de LLAMA.PE antes de ser publicado, y se controlan las versiones del mismo, a fin de evitar modificaciones y suplantaciones no autorizadas.

# 13 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

Validación de Certificados

https://llama.pe/repository

## 13.1 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/repository

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.

## 13.2 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 mediante su página web la lista de certificados revocados con una periodicidad diaria. Cabe destacar que se publicará la última CRL.

- 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.

## 13.3 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.

# 14 IDENTIFICACION Y AUTENTICACION

## 14.1 NOMBRES

### 14.1.1 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.

### 14.1.2 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”.

### 14.1.3 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.

### 14.1.4 REGLAS PARA LA INTERPRETACIÓN DE VARIAS FORMAS DE NOMBRE

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

### 14.1.5 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.

### 14.1.6 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.

# 15 VALIDACIÓN INICIAL DE LA IDENTIDAD

## 15.1 MÉTODO PARA DEMOSTRAR LA POSESIÓN DE LA CLAVE PRIVADA

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

1. Generación de claves por parte de la EC

En Software, se entregan al Suscriptor en mano o mediante correo mediante 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.

2. Generación de las claves por 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.

## 15.2 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.

## 15.3 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.

## 15.4 INFORMACIÓN DE TITULAR NO VERIFICADA

Bajo ninguna circunstancia la EC del 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.

Puede realizar auditorías o monitoreo del servicio para cumplimiento de LA CP y CPS.

## 15.5 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 de Prácticas de Registro o Verificación de LLAMA.PE – RPS.

## 15.6 CRITERIOS PARA LA INTEROPERABILIDAD

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

# 16 IDENTIFICACIÓN Y AUTENTICACIÓN PARA PETICIONES DE RE-EMISIÓN DE CLAVES

## 16.1 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 renovación y con base en ello emite los certificados digitales.

Los procedimientos de autenticación son descritos en el documento de Declaración de Prácticas de Registro o Verificación de LLAMA.PE – RPS.

## 16.2 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 de Prácticas de Registro o Verificación de LLAMA.PE – RPS.

# 17 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 de Prácticas de Registro o Verificación de LLAMA.PE – RPS, 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.

# 18 REQUISITOS OPERACIONALES PARA EL CICLO DE VIDA DE LOS CERTIFICADOS

## 18.1 SOLICITUD DEL CERTIFICADO

Dicho procedimiento le compete a la Entidad de Registro y por lo tanto se describe en el documento Declaración de Prácticas de Registro o Verificación de LLAMA.PE – RPS.

## 18.2 QUIÉN PUEDE SOLICITAR UN CERTIFICADO

Los procedimientos relativos a la Entidad de Registro son descritos en el documento de Declaración de Prácticas de Registro o Verificación de LLAMA.PE – RPS.

## 18.3 PROCESO DE REGISTRO Y RESPONSABILIDADES

Los procedimientos relativos a la Entidad de Registro son descritos en el documento de Declaración de Prácticas de Registro o Verificación de LLAMA.PE – RPS.

# 19 TRAMITACIÓN DE SOLICITUD DE CERTIFICADOS

## 19.1 REALIZACIÓN DE LAS FUNCIONES DE IDENTIFICACIÓN Y AUTENTICACIÓN

Los procedimientos relativos a la Entidad de Registro son descritos en el documento de Declaración de Prácticas de Registro o Verificación de LLAMA.PE – RPS.

## 19.2 APROBACIÓN O RECHAZO DE LAS SOLICITUDES DE CERTIFICADO

Los procedimientos relativos a la Entidad de Registro son descritos en el documento de Declaración de Prácticas de Registro o Verificación de LLAMA.PE – RPS.

## 19.3 PLAZO PARA PROCESAR LAS SOLICITUDES DE CERTIFICADO

Los procedimientos relativos a la Entidad de Registro son descritos en el documento de Declaración de Prácticas de Registro o Verificación de LLAMA.PE – RPS.

# 20 EMISIÓN DE CERTIFICADOS

## 20.1 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.

LLAMA.PE realiza la emisión procediendo de la siguiente manera:

### 20.1.1 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.

### 20.1.2 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.

### 20.1.3 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.

## 20.2 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.

# 21 ACEPTACIÓN DEL CERTIFICADO

## 21.1 FORMA EN LA QUE SE ACEPTA EL CERTIFICADO

Los procedimientos relativos a la Entidad de Registro son descritos en el documento de Declaración de Prácticas de Registro o Verificación de LLAMA.PE – RPS.

## 21.2 PUBLICACIÓN DEL CERTIFICADO POR LA EC

Los procedimientos relativos a la Entidad de Registro son descritos en el documento de Declaración de Prácticas de Registro o Verificación de LLAMA.PE – RPS.

## 21.3 NOTIFICACIÓN DE LA EMISIÓN DEL CERTIFICADO POR LA EC A OTRAS ENTIDADES

Los procedimientos relativos a la Entidad de Registro son descritos en el documento de Declaración de Prácticas de Registro o Verificación de LLAMA.PE – RPS.

# 22 USO DE LA CLAVE PRIVADA Y DEL CERTIFICADO

## 22.1 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 Titular/Suscriptor identifica las obligaciones con respecto a la Protección de Clave Privada.

Las claves privadas sólo se deben utilizar de manera responsable tal cual se indica en la RPS de Llama.pe y durante el tiempo de vigencia que puede ser de 3 años como máximo.

Al final de la vida útil de una clave privada, los Titular/Suscriptor deben eliminar de forma segura la clave privada y los fragmentos que se han dividido para fines de copia de seguridad.

## 22.2 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.

# 23 RENOVACIÓN DEL CERTIFICADO SIN CAMBIO DE CLAVES

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

# 24 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 dos meses antes de la expiración del certificado, para que pueda renovar a tiempo dicho certificado.

Se cuenta con alertas para la renovación de 2 meses, un mes, 15 días, 7 dias, 1 día antes de la expiración del 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.

## 24.1 CIRCUNSTANCIAS PARA LA RE-EMISIÓN DE CERTIFICADOS CON CAMBIO DE CLAVES

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

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

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

## 24.3 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 de Prácticas de Registro de LLAMA.PE como Entidad de Registro.

## 24.4 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 de Prácticas de Registro de LLAMA.PE como Entidad de Registro.

## 24.5 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 de Prácticas de Registro de LLAMA.PE como Entidad de Registro.

## 24.6 PUBLICACIÓN DEL CERTIFICADO RE-EMITIDO POR LA EC

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

## 24.7 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 de Prácticas de Registro de LLAMA.PE como Entidad de Registro.

# 25 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.

# 26 REVOCACIÓN Y SUSPENSIÓN DE CERTIFICADOS

## 26.1 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.

## 26.2 QUIÉN PUEDE SOLICITAR UNA REVOCACIÓN

La revocación de un certificado podrá solicitarse por:

- El titular/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.

## 26.3 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.

## 26.4 PERIODO DE GRACIA DE SOLICITUD DE REVOCACIÓN

No aplica.

## 26.5 PLAZO EN EL QUE LA EC DEBE RESOLVER LA SOLICITUD DE REVOCACIÓN

Los procedimientos relativos a la Entidad de Registro son descritos en el documento de Declaración de Prácticas de Registro o Verificación de LLAMA.PE – RPS.

## 26.6 REQUISITOS DE VERIFICACIÓN DE LAS REVOCACIONES POR LOS TERCEROS QUE CONFÍAN

Los procedimientos relativos a la Entidad de Registro son descritos en el documento de Declaración de Prácticas de Registro o Verificación de LLAMA.PE – RPS.

## 26.7 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.

## 26.8 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.

## 26.9 DISPONIBILIDAD DE VERIFICACIÓN DEL ESTADO

La información relativa a la CRL estará disponible en línea con un mínimo de 99% anual.

## 26.10 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 EC LLAMA.PE y que sea la última Lista emitida.

## 26.11 OTRAS FORMAS DISPONIBLES DE DIVULGACIÓN DE INFORMACIÓN DE REVOCACIÓN

No aplica

## 26.12 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.

## 26.13 CIRCUNSTANCIAS PARA LA SUSPENSIÓN

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

# 27 SERVICIOS DE INFORMACIÓN DEL ESTADO DE CERTIFICADOS

## 27.1 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.

## 27.2 DISPONIBILIDAD DEL SERVICIO

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

# 28 FINALIZACIÓN DE SUSCRIPCIÓN

La finalización de los acuerdos del suscriptor con la Entidad de Certificación se realiza cuando el certificado expira o se revoca.

# 29 ALMACENAMIENTO Y RECUPERACIÓN DE LA CLAVE (CERTIFICADOS DE CIFRADO)

Llama.pe no emite certificados con atributo de cifrado, únicamente con atributo de no repudio y firma digital. El código de las políticas de certificación se encuentran definidas en la sección 6.3 del presente documento.

# 30 CONTROLES FÍSICOS DE LA INSTALACIÓN, GESTIÓN, COMPUTACIONALES Y OPERACIONALES

Los controles físicos de seguridad se encuentran descritos en la CPS de Llama.pe.

# 31 CONTROLES TÉCNICOS DE SEGURIDAD

Los controles técnicos de seguridad se encuentran descritos en la CPS de Llama.pe.

# 32 CAMBIO DE CLAVES

Ver sección Re-emisión del certificado.

# 33 AUDITORÍA DE CONFORMIDAD Y OTROS CONTROLES

Las directrices para la realización de auditorías se encuentran descritas en la CPS de Llama.pe. Se conserva la información de los registros de acuerdo a lo solicitado a la legislación.

# 34 COMPROMISO DEL RECUPERACION DE DESASTRES

Se describe en la CPS del LLAMA.pe

# 35 FINALIZACIÓN DE EC

Se describe en la CPS del LLAMA.pe

# 36 GENERACIÓN E INSTALACIÓN DEL PARA DE LLAVES

Se describe en la CPS del LLAMA.pe

# 37 PROTECCIÓN DE LA CLAVE PRIVADA

Se describe en la CPS del LLAMA.pe

# 38 DESTRUCCIÓN DE LAS CLAVES

Se describe en la CPS del LLAMA.pe

# 39 DATOS DEL ACTIVACION

Se describe en la CPS del LLAMA.pe

# 40 PERFILES DE CERTIFICADOS, OSCP Y CRL

## 40.1 PERFIL DE CERTIFICADO

Todos los certificados emitidos bajo esta política serán conformes al estándar X.509 versión 3 y al RFC 3039 "Internet X.509 Public Key Infrastructure Qualified Certificates Profile".

## 40.2 NÚMERO DE VERSIÓN

LLAMA.PE emite certificados X.509 Versión 3.

### 40.2.1 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.

### 40.2.2 EXTENSIÓN CON LAS FACULTADES DE REPRESENTACIÓN ESPECIAL

El certificado, emitido bajo la presente Política, 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.

### 40.2.3 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.

### 40.2.4 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.

### 40.2.5 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.

## 40.3 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.

### 40.3.1 NÚMERO DE VERSIÓN

El formato de las CRLs utilizadas es el especificado en la versión 2 (X509 v2).

### 40.3.2 CRL Y EXTENSIONES CRL

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

## 40.4 PERFIL DE OSCP

El perfil del certificado de OSCP está realizado de acuerdo a RFC 6060

# 41 OTROS ASUNTOS LEGALES Y COMERCIALES

## 41.1 CONFIDENCIALIDAD DE LA INFORMACIÓN COMERCIAL

### 41.1.1 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 59/2003, de Firma Electrónica (artículo 19.3) como documento de seguridad.

### 41.1.2 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.

## 41.2 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.

# 41.3 OBLIGACIONES

## 41.3.1 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.

## 41.3.2 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.

## 41.3.3 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.

## 41.3.4 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.

### 41.3.5 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.

### 41.3.6 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.

### 41.3.7 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.

## 41.4 VIGENCIA Y CONCLUSIÓN

La CP y CPS se encuentran vigentes desde el momento de su publicación y hasta la aprobación de una nueva versión del mismo o cuando haya culminado sus operaciones., los cuales están publicados en el repositorio del LLAMA.pe

Se cuenta con un histórico de versiones de las CP y CPS, disponible a solicitud del cliente.

Todos los involucrados y participantes deben cumplir lo descrito en la CP y CPS, contando con el servicio disponible siempre que se cuente con certificados vigentes

## 41.5 CONCLUSIONES Y ENMIENDAS

CP y/o CPS puede ser actualizada y el impacto de los cambios es revisado por el personal que administra la CP y/o CPS.

SI producto de la actualización de CP y/o CPS afecta o perjudica a terceros que confían, se puede asignar un nuevo OID a la documentación actualizada.

De actualizar la CP y/o CPS, estos deben serán publicados en la página Web

## 41.6 RESOLUCIÓN DE DISPUTAS

Para la resolución de disputas se escribe un correo electrónico brindado por el suscriptor/titular con los argumentos de la disputa en mención al correo electrónico de la ENTIDAD soporte@llama.pe del ser de su ámbito.

# 42 CLÁUSULAS MISCELÁNEAS

## 42.1 ACUERDO INTEGRO

La EC contará con un documento que establece un acuerdo entre las partes, el cual reemplaza a los acuerdos previos y contemporáneos del ser requerido.

## 42.2 ASIGNACIÓN

La EC limita el uso del certificado digital del titular/suscriptor de acuerdo a lo estipulado a la CP y/o CPS.

## 42.3 DIVISIBILIDAD

El documento contractual que se brindará al titular/suscriptor cuenta con cláusulas independientes basado en la CP y CPS, estas no se afectan unas con otras, por tal motivo una cláusula no podrá invalidar a otra en caso de adición, omisión o modificaciones, excepto previo acuerdo con el suscriptor/titular.

## 42.4 EJECUCIÓN

De llegar a alguna disputa o incumplimiento entre las partes, los costos incluido el honorario de abogados será asumida por cada parte.

## 42.5 FUERZA MAYOR

La Entidad limita su responsabilidad en caso fortuito y en caso de fuerza mayor, en las condiciones generales de emisión y uso del certificado.

# 43 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 -Ley27269, para el reconocimiento legal de los servicios emitidos bajo las directrices definidas en el presente documento.

# 44 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