DECLARACIÓN E IMPLEMENTACIÓN DE PRÁCTICAS DE FIRMA REMOTA

VERSIÓN: V1.1

PUBLICO

OFICIAL

FR-DPFR-001

PARA: LLAMA.PE

HISTORIAL DE VERSIONES

VERSIÓN	DESCRIPCIÓN	REALIZADO POR	FECHA DE APROBACIÓN	FECHA DE REVISIÓN
V1.1	se actualiza el punto 5 de aplicabilidad, 12 frecuencia de publicación, 11.6 conformidad con la ley aplicable, 6.4 responsabilidades de los terceros que confían,	LOUIE DIAZ MARTICORENA	2025-10-22	2025-10-22
V1.0	version inicial	LOUIE DIAZ MARTICORENA	2025-08-22	2025-08-22

Documentos de Herencia

No tiene documentos de herencia.

Documentos de Referencia

No tiene documentos de referencia.

Tabla de contenido

1 INTRODUCCIÓN

Esta DPFR establece las prácticas que lleva a cabo "LLAMA.PE". para emitir, gestionar, revocar y renovar certificados digitales en su modalidad de firma remota

2 OBJETIVO

Establecer de manera clara y pública las políticas, procedimientos y controles aplicables a la prestación del servicio de firma remota, asegurando que estas prácticas se implementen efectivamente y cumplan con los estándares regulatorios y de seguridad exigidos por el marco legal peruano y la Guía de Acreditación.

3 DEFINICIONES

- **Agente automatizado:** Procesos y dispositivos programados para atender solicitudes previamente definidas y ofrecer respuestas automáticas sin intervención humana en esa etapa.
- **Archivo:** Conjunto ordenado de documentos generados o recibidos por una entidad en el ejercicio de sus funciones, destinados a servir de referencia o consulta.
- **Archivo electrónico:** Conjunto de registros relacionados entre sí, así como la forma organizada en que estos se almacenan.
- **Aplicabilidad o propósito de un certificado:** Ámbito de uso permitido para un certificado digital dentro de una comunidad específica.
- **Autenticación:** Procedimiento técnico que permite verificar la identidad de la persona que firma electrónicamente, vinculando su firma con el mensaje firmado. No implica certificación notarial ni fe pública.
- **Autoridad Administrativa Competente:** Organismo estatal encargado de acreditar a las Entidades de Certificación, Entidades de Registro o Verificación y Prestadores de Servicios de Valor Añadido, así como de reconocer estándares tecnológicos de la Infraestructura Oficial de Firma Electrónica, supervisar su funcionamiento y ejercer las funciones asignadas por el reglamento u otras necesarias en sus operaciones.
- **Canal seguro:** Medio físico o virtual independiente que permite la transmisión de datos de forma confidencial y confiable, evitando su interceptación o alteración por terceros.
- **Certificado digital:** Documento electrónico, emitido y firmado digitalmente por una Entidad de Certificación, que asocia un par de claves con una persona natural o jurídica confirmando su identidad.
- **Suspensión:** Acción de desactivar temporalmente la validez de un certificado digital por un plazo determinado, sin exceder su fecha de expiración.
- **Clave privada:** Clave de un sistema de criptografía asimétrica utilizada para generar firmas digitales sobre documentos electrónicos y que debe ser mantenida en secreto por su titular.
- **Clave pública:** Clave complementaria en criptografía asimétrica, utilizada para verificar la firma digital de un documento. Puede ser conocida por cualquier persona.
- **Código de verificación o resumen (hash):** Secuencia de bits de longitud fija generada por un algoritmo aplicado a un documento electrónico, cumpliendo con que:
- Siempre produzca el mismo resultado para el mismo documento.
- No sea factible reconstruir el documento a partir del código.
- Sea improbable encontrar dos documentos distintos con el mismo código usando el mismo algoritmo.
- **Criptografía asimétrica:** Rama de las matemáticas aplicadas que transforma documentos electrónicos en formatos ilegibles y permite devolverlos a su forma original mediante el uso de dos claves distintas pero relacionadas: la clave privada para firmar o cifrar, y la clave pública para verificar o descifrar. La relación entre ambas no permite obtener la privada a partir de la pública.
- **Declaración de Prácticas de Valor Añadido:** Documento presentado por una Entidad de Registro o Verificación a la Autoridad Administrativa Competente, en el que detalla los procedimientos y prácticas empleadas en la prestación de sus servicios.
- **Depósito de certificados:** Sistema que permite almacenar y recuperar certificados y la información asociada, disponible a través de medios telemáticos.
- **Documento electrónico:** Unidad estructurada de información, publicada o no, que puede ser creada, organizada, gestionada, transmitida, procesada o conservada por personas u organizaciones mediante sistemas informáticos, según sus necesidades funcionales.

- **Entidad de certificación (EC):** Persona jurídica, pública o privada, que ofrece servicios relacionados con la certificación digital, como producción, emisión, gestión o cancelación, pudiendo también desempeñar funciones de registro o verificación.
- **Entidad de Registro o Verificación (ER):** Persona jurídica, distinta de los notarios, que se encarga de recopilar y verificar los datos de quienes solicitan un certificado digital, autorizar su emisión o cancelación, siguiendo la normativa vigente y bajo supervisión correspondiente.
- **Estándares técnicos nacionales:** Normas técnicas oficiales aprobadas como Normas Técnicas Peruanas por la Comisión de Normalización y Fiscalización de Barreras Comerciales no Arancelarias del INDECOPI, en su rol de Organismo Nacional de Normalización.
- **Firma remota**: La firma remota en el Perú es una modalidad de firma digital que permite a una persona firmar documentos electrónicos desde cualquier dispositivo, usando certificados digitales custodiados en un servidor seguro acreditado por Indecopi, con plena validez legal equivalente a la firma manuscrita.
- **Gobierno electrónico:** Uso de las Tecnologías de Información y Comunicación para redefinir la relación entre el Estado, la ciudadanía y las empresas, optimizar la gestión y los servicios, fomentar la transparencia y participación, y asegurar el acceso seguro a la información pública, apoyando la integración y desarrollo de distintos sectores.
- **Hardware:** Conjunto de componentes físicos que forman parte de una computadora o sistema tecnológico, término originado del inglés y definido por la RAE. Se usa de forma general para referirse a elementos materiales de una tecnología.
- **Identificador de objeto (OID):** Secuencia numérica definida según el estándar ASN.1 que identifica de forma única un objeto. En certificación digital, se usa para identificar elementos como componentes de nombres diferenciados o documentos de políticas (CPS).

4 PARTICIPANTES

AUTORIDAD ADMINISTRATIVA COMPETENTE: Es el organismo público responsable de acreditar de reconocer los estándares tecnológicos aplicables en la Infraestructura Oficial de Firma Electrónica, de supervisar dicha Infraestructura, y las otras funciones señaladas en el presente Reglamento o aquellas que requiera en el transcurso de sus operaciones.

ENTIDAD DE CERTIFICACIÓN LLAMA.PE (EC LLAMA.PE): LLAMA.PE, en su papel de Entidad de Certificación acreditada, es la persona jurídica privada que presta indistintamente servicios de producción, emisión, gestión u otros servicios inherentes a la certificación digital.

ENTIDAD DE REGISTRO LLAMA.PE (ER LLAMA.PE) LLAMA.PE, en su papel de Entidad de certificación acreditada, es la persona jurídica privada que realiza la identificación y validación de los solicitantes de certificados digitales, asegurando la confianza y seguridad en el proceso de firma electrónica

WATANA: Software de firma acreditado de LLAMA.PE, esencial para la generación de la firma remota

TITULAR : Es la persona natural o jurídica a quien se le atribuye de manera exclusiva un certificado digital. (*Guía de Acreditación de Entidad de Registro V.4.0*)

SUSCRIPTOR: Es la persona natural responsable de la generación y uso de la clave privada, a quien se le vincula de manera exclusiva con un documento electrónico firmado digitalmente utilizando su clave privada. (*Guía de Acreditación de Entidad de Registro V.4.0*)

- Tratándose de personas naturales, éstas son titulares y suscriptores del certificado digital.
- En el caso de personas jurídicas, éstas son titulares del certificado digital. Los suscriptores son las personas naturales responsables de la generación y uso de la clave privada, con excepción de los certificados digitales para su utilización a través agentes automatizados, situación en la cual las personas jurídicas asumen las facultades de titulares y suscriptores del certificado digital.

TERCERO QUE CONFÍA O TERCER USUARIO: Se refiere a las personas naturales, equipos, servicios o cualquier otro ente que actúa basado en la confianza sobre la validez de un certificado y/o verifica alguna firma digital en la que se utilizó dicho certificado.

5 APLICABILIDAD

Esta sección establece el alcance del documento – ¿a qué se aplica, qué servicios y qué tipos de certificados, y bajo qué condiciones se aplica?

Esta Declaración e Implementación de las Prácticas se aplica a todos los procesos, servicios, procedimientos, roles, controles y firmas de los certificados emitidos bajo la infraestructura de certificación digital de la organización (o jerarquía) que implementa la IOFE conforme a la Ley N.º 27269 – Ley de Firmas y Certificados Digitales y su reglamento.

Alcance específico incluye:

- Emisión, gestión, renovación, revocación, suspensión, expiración de certificados digitales.
- Publicación de certificados y listas de revocación (CRL) o mecanismos equivalentes.
- Servicios de confianza adicionales (por ejemplo: sellado de tiempo, autenticación, cifrado) asociados a los certificados emitidos.
- Entidades que participan en dicha jerarquía (AC principal, subordinadas, ER, suscriptores, terceros que confían).
- El Documento no aplica para certificados que caen fuera del marco de la IOFE o que no están sujetos al control de acreditación de la AAC.
- No aplica a servicios internos no orientados a terceros o que no impliquen emisión de certificados reconocidos públicamente.
- Aplica en el territorio de la República del Perú o en las jurisdicciones que se reconozcan mutuamente conforme a los convenios vigentes para firma digital.

6 RESPONSABILIDADES Y OBLIGACIONES

6.1 RESPONSABILIDADES Y OBLIGACIONES DEL TITULAR

El titular es la persona a la que se le atribuye de manera exclusiva un certificado digital que contiene una firma digital, identificándolo objetivamente en relación con el mensaje de datos (art. 4, ley 27269). Para ser titular de un certificado digital adicionalmente se deberá cumplir con entregar la información solicitada por la Entidad de Registro o Verificación, de acuerdo a lo estipulado por la Entidad de Certificación correspondiente, asumiendo el titular la responsabilidad por la veracidad y exactitud de la información proporcionada, sin perjuicio de la respectiva comprobación. En el caso de personas naturales, la solicitud del certificado digital y el registro o verificación de su identidad son estrictamente personales. La persona natural solicitante se constituirá en titular y suscriptor del certificado digital. (art. 13, D.S 052-2008-PCM)

6.2 RESPONSABILIDADES Y OBLIGACIONES DEL SUSCRIPTOR

Dentro de la Infraestructura Oficial de Firma Electrónica, la responsabilidad sobre los efectos jurídicos generados por la utilización de una firma digital corresponde al titular del certificado. Tratándose de personas naturales, éstas son titulares y suscriptores del certificado digital. En el caso de personas jurídicas, éstas son titulares del certificado digital. Los suscriptores son las personas naturales responsables de la generación y uso de la clave privada, con excepción de los certificados digitales para su utilización a través agentes automatizados, situación en la cual las personas jurídicas asumen las facultades de titulares y suscriptores del certificado digital. (art.9 D.S 052-2008-PCM)

Las obligaciones del suscriptor son: (art.10 D.S 052-2008-PCM)

- Entregar información veraz bajo su responsabilidad. Generar por sí mismo la clave privada, o autorizar su generación a distancia por parte de un Prestador de Servicios de Valor Añadido acreditado en la modalidad de sistema de creación de firma remota, y firmar digitalmente mediante los procedimientos señalados por la Entidad de Certificación.
- Mantener el control y la reserva del pin de autorización en WATANA app (esto porque la responsabilidad del Prestador de Servicios de Valor Añadido acreditado en la modalidad de firma remota custodia la clave privada en el equipo criptográfico HSM CP5.
- Observar las condiciones establecidas por la Entidad de Certificación para la utilización del certificado digital y la generación de firmas digitales.
- En caso de que el pin de autorización o el aplicativo de WATANA app se vean comprometida en su seguridad, el suscriptor debe notificarlo de inmediato a la Entidad de Registro o Verificación o a la Entidad de Certificación que participó en su emisión para que

proceda a la cancelación del certificado digital.

6.3 RESPONSABILIDADES Y OBLIGACIONES DE LLAMA.PE

Llama.pe dispondrá en todo momento de una póliza de seguro en los términos que marque la legislación vigente. Llama.pe 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.

Llama.pe 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:

- La exactitud de toda la información contenida en el certificado en la fecha de su emisión.
- La garantía de que, en el momento de la entrega del certificado, obra en poder LLAMA.PE la clave privada, siendo este generado y almacenado en el HSM Utimaco CryptoServer CP5 sin posibilidad alguna de su extracción.
- La garantía de que la clave pública y privada funcionan conjunta y complementariamente.
- La correspondencia entre el certificado solicitado y el certificado entregado.
- Cualquier responsabilidad que se establezca por la legislación vigente.

6.3.1 RESOLUCION DE DISPUTAS

Para la resolución de disputas el titular/suscriptor escribe desde el correo electrónico soporte@llama.pe con los argumentos de la disputa en mención 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.

6.4 RESPONSABILIDADES DE LOS TERCEROS QUE CONFIAN

Los Terceros que confían son personas naturales o jurídicas que aceptan y confían en la validez de un certificado digital emitido por la Autoridad de Certificación, con el fin de verificar una firma electrónica, autenticar la identidad de un firmante, cifrar información, o validar transacciones electrónicas.

Los terceros que confían asumen las siguientes responsabilidades:

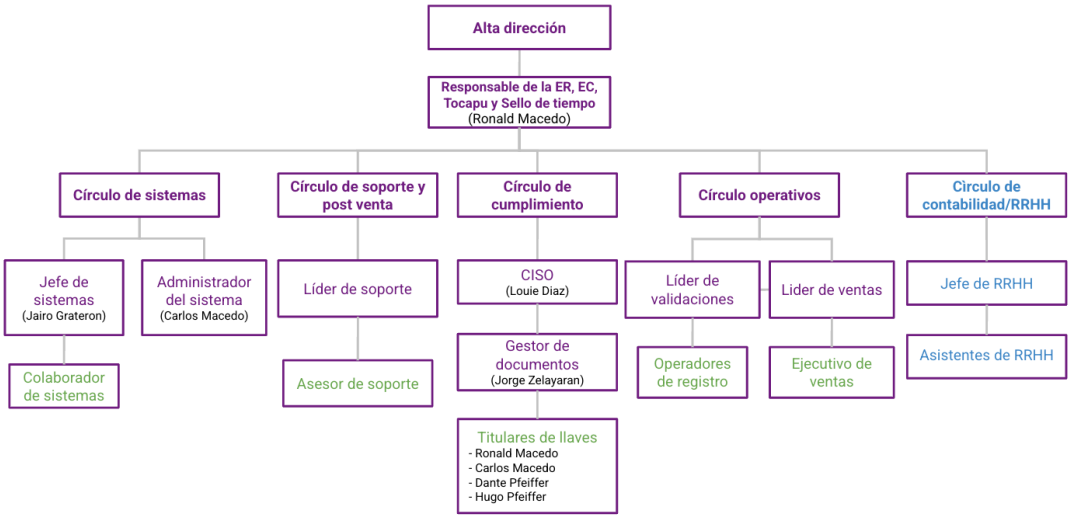
- Comprobar que el certificado presentado esté vigente, no revocado ni suspendido, consultando los mecanismos de validación provistos por la AC (por ejemplo, CRL, OCSP u otro medio autorizado).
- Verificar la integridad de la cadena de certificación hasta la raíz confiable de la Infraestructura Oficial de Firma Electrónica (IOFE).
- Revisar la Política de Certificación (PC) y la Declaración de Prácticas de Certificación (CPS) aplicables al certificado que utilizan, para asegurarse de entender sus límites de uso, garantías, niveles de seguridad y restricciones.
- Utilizar los certificados solo para los fines indicados en la Política de Certificación correspondiente (por ejemplo, autenticación, firma digital, cifrado o sellado de tiempo).
- No usar el certificado para fines prohibidos, ilícitos o no previstos en la PC o CPS.
- Validar técnicamente la firma digital y el certificado mediante software o sistemas de validación debidamente acreditados.
- Reconocer que la confianza en el certificado debe estar limitada al nivel de seguridad declarado por la AC y a la finalidad prevista del certificado.

7. GESTIÓN DEL CLICO DE VIDA DE LAS CLAVES

El ciclo de vida de los certificados digitales generados desde un HSM Utimaco CP5 configurado para firma remota inicia con la generación segura del par de claves dentro del propio HSM, garantizando que la clave privada no abandona nunca el dispositivo, conforme a los requisitos de un dispositivo cualificado de creación de firma (QSCD). Una vez emitido el certificado, este entra en su fase operativa, siendo utilizado exclusivamente para procesos de firma digital remota bajo el control de un módulo SAM (Signature Activation Module). Durante su vigencia, el certificado puede ser revocado si se detecta algún compromiso de seguridad o por razones administrativas. Al alcanzar la

fecha de expiración establecida en la política de certificación, el certificado es dado de baja y eliminado del HSM de acuerdo con el procedimiento interno de eliminación segura, garantizando así la integridad y el cumplimiento normativo del sistema de firma.

8 GESTION DE SEGURIDAD



8.1 ORGANIZACION DE LA SEGURIDAD DE LA INFORMACIÓN

LLAMA.PE tiene designado a un Responsable de la Entidad quien al mismo tiempo es el representante de la empresa; también la empresa cuenta con la designación de un Oficial de seguridad quien es responsable de seguridad y privacidad de datos personales de LLAMA.PE, gestiona la implementación y vela por el cumplimiento de la presente política, así como de su revisión periódica, actualización, difusión y concientización y capacitación al personal y terceros para su adecuado cumplimiento.

8.2 POLITICA DE SEGURIDAD DE LA INFORMACIÓN

La politica de seguridad tiene como objetivo la descripción de operaciones y prácticas de seguridad de la información que cumple LLAMA.PE para la administración de sus servicios como V.A en la modalidad de firma remota dentro de la infraestructura de la EC; en el marco del cumplimiento de los requerimientos de las Guías de Acreditación establecidas por el INDECOPI. Aunque la EC y la firma remota no comparten el mismo HSM si pertenecen a la misma infraestructura y procedimiento de emisión de certificado variando solo en el tema del almacenamiento; dichos servicios comparten las mismas prácticas de seguridad de la información.

Esta política se centra en tres aspectos críticos: la Confidencialidad, la Integridad y la Disponibilidad de la información. Nos comprometemos a proteger la privacidad y el acceso a la información, garantizando su autenticidad y su accesibilidad cuando sea necesario. Además, gestionamos proactivamente los riesgos de seguridad de la información al identificar posibles amenazas y estableciendo medidas preventivas para mitigarlas. Asimismo, estamos preparados para responder de inmediato a cualquier violación de seguridad de la información detectada en la empresa, con el objetivo de minimizar el impacto y prevenir futuros incidentes.

8.3 SEGURIDAD EN EL TRATO CON 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 podrían 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, 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.

En cuanto a la gestión de la entrega de servicios de terceros, se tiene en cuenta lo siguiente:

- Entrega del servicio: LLAMA.PE verifica que el servicio brindado por el tercero sea tal y como el propuesto en el Contrato Marco de Servicios y sus respectivos anexos.
- Monitoreo y revisión del servicio: LLAMA.PE tiene la facultad de solicitar al tercero reportes o informes con respecto al servicio brindado. Asimismo, las auditorías internas y externas que se realizan semestral y/o anualmente pueden requerir la visita de las instalaciones de terceros.
- Cambios en el servicio: LLAMA.PE se encarga de gestionar los cambios en la provisión del servicio, incluyendo mantenimiento y mejoras en el presente documento.

8.4 SEGURIDAD DEL PERSONAL

Llama.pe al contar con su certificación ISO 27001:2022 aplica a los controles del anexo A (ISO 27002) en los cuales se encuentra el control **6 Controles de personal,** dentro de los cuales se han implementados controles:

8.4.1 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.

En general, LLAMA.PE retirará de sus funciones de confianza a un empleado cuando se tenga conocimiento de la existencia de la comisión de algún hecho delictivo que pudiera afectar al desempeño de sus funciones o dañe la reputación de la EC. LLAMA.PE no asignará a un sitio confiable o de gestión a una persona que no sea idónea para el puesto, especialmente por haber sido condenada por delito o falta que afecte su idoneidad para el puesto.

8.4.2 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. Llama.pe puede requerir otros tipos de comprobación de antecedentes, dependiendo del rol a contratar

8.4.3 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 las prácticas de EC.

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.

8.4.4 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 los servicios
- Oficiales de seguridad: Responsables de administrar la implementación de las prácticas de seguridad

- Administradores de sistemas: Autorizados a instalar, configurar y mantener la integridad de los sistemas del SVA
- Jefe de de sistemas: Responsable de operar la integridad de los sistemas en el día a día. Autorizados para ejecutar sistemas de respaldo y recuperación.
- Titulares de las claves (4)

8.5 SEGURIDAD FISICA Y DEL ENTORNO

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.

8.5.1 UBICACION FISICA

El HSM CP5 se encuentra alojado en un centro de datos en el Perú que cuenta con certificaciones internacionales clave para garantizar alta disponibilidad y continuidad del servicio.

El centro de datos cuenta con certificación Tier III Certification of Design del Uptime Institute, lo cual valida que su infraestructura está diseñada según los más exigentes estándares globales. Esta certificación implica que el centro soporta tareas de mantenimiento y reemplazo de componentes sin interrumpir la operación; además dispone de una configuración N+2 Catcher, que proporciona redundancia adicional en componentes críticos y permite asegurar la continuidad operativa ante cualquier eventualidad.

Cuentan con Carrier-neutral que permite conectividad con múltiples operadores locales e internacionales, evitando la dependencia de un único proveedor y reduciendo riesgos de caída por falla de red. Incorporan detección temprana de incendios, extinción automática, control de acceso riguroso y videovigilancia operativa 24/7, garantizando protección contra amenazas físicas. En relación al los sistemas de energía y clima redundantes cuantas con energía tolerante a fallos, climatización simultánea (aire acondicionado y refrigeración líquida), y diseño modular “box-in-a-box” que mejora aislamiento térmico y eficiencia. A continuación se detallas las certificaciones internacionales y gestión de riesgos:

- ISO 9001 (Gestión de Calidad)
- ISO 22301 (Continuidad del Negocio) – certificado en Lima desde 2024
- ISO 27001, 27017, 27018, 27701 (Seguridad de la Información, nube y privacidad) – desde 2018 a 2024
- ISO 20000-1 (Gestión de servicios TI)
- Conformidad con SOC 1, SOC 2, SOC 3 y PCI-DSS, que respaldan la integridad operativa y la protección de datos transaccionales

8.5.2 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.

8.5.3 ALIMENTACIÓN ELÉCTRICA Y AIRE ACONDICIONADO

En relación al los sistemas de energía y clima redundantes cuantas con energía tolerante a fallos, climatización simultánea (aire acondicionado y refrigeración líquida), y diseño modular “box-in-a-box” que mejora aislamiento térmico y eficiencia.

8.5.4 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.

8.6 MANEJO DE MEDIOS

El manejo del HSM CP5 se realiza bajo estrictos protocolos de seguridad física y operativa, considerando que se trata de un equipo criptográfico de alta sensibilidad y con un rol crítico en la custodia de llaves privadas. Solo personal autorizado y debidamente capacitado debe manipular el dispositivo, utilizando procedimientos documentados que incluyan el registro de cada intervención y la verificación dual (principio de doble control). Durante su instalación o mantenimiento, el HSM debe permanecer en áreas restringidas, con acceso controlado y monitoreo permanente, minimizando así la exposición a riesgos de manipulación no autorizada o daños accidentales.

En cuanto a su traslado, este se realiza en embalajes especializados que protejan al equipo de golpes, vibraciones, humedad y descargas electrostáticas. El transporte debe realizarse de manera directa y segura, preferentemente bajo custodia y utilizando rutas previamente planificadas para reducir riesgos. Estas medidas garantizan que la integridad y confiabilidad del HSM no se vean comprometidas en ninguna etapa de su ciclo de vida operativo.

8.7 PLANIFICACIÓN DEL SISTEMA

Dentro de la operación de la plataforma de firma remota, el uso de EJBCA permite realizar un monitoreo continuo sobre el desempeño y la capacidad del HSM, asegurando que este mantenga niveles adecuados de procesamiento criptográfico frente a la demanda de transacciones. EJBCA ofrece métricas y registros de actividad que permiten observar en tiempo real el número de operaciones ejecutadas, el tiempo de respuesta en la generación y validación de firmas digitales, así como alertas relacionadas con el consumo de recursos del HSM. Esta supervisión constante constituye una base para identificar tendencias de uso y posibles cuellos de botella antes de que afecten la disponibilidad del servicio.

Adicionalmente, los reportes generados a través de EJBCA facilitan la proyección de la demanda futura al permitir correlacionar el crecimiento en las solicitudes de firma con la capacidad de procesamiento del HSM. Estos datos permiten planificar de manera preventiva ajustes en la infraestructura, tales como la optimización de configuraciones o la eventual incorporación de nuevos recursos, garantizando que el servicio de firma remota se mantenga disponible y con tiempos de respuesta consistentes. De esta manera, el monitoreo integrado de EJBCA asegura no solo la continuidad operativa, sino también una gestión proactiva de la capacidad del HSM.

8.8 REPORTE Y RESPUESTA A INCIDENCIAS

LLAMA.PE cuenta con los siguiente documentos para realizar una gestión de las incidencias:

- LN-MET-001 METODOLOGÍA DE GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN
- LN-POL-008 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN
- LN-PRO-003 PROCEDIMIENTO DE GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION

8.8.1 ROLES QUE PARTICIPAN EN EL PROCESO

Gerencia

En caso de llegar a requerirse y hacerse la valoración económica del activo de información involucrado en un evento/incidente de seguridad de la información, aprueba los presupuestos financieros necesarios para la adquisición de activos y servicios para erradicar las causas del incidente.

Oficial de Seguridad de la Información

Orienta el adecuado tratamiento a los incidentes de seguridad de la información detectados o reportados.

Debe hacer un seguimiento periódico a los incidentes de seguridad presentados.

Trabajadores y colaboradores

Tomar conciencia de su responsabilidad de reportar eventos y debilidades de seguridad de la información tan pronto como sea posible.

Reportar oportunamente los incidentes o eventos de seguridad de la información y cualquier comportamiento anormal que se presente en la empresa o en sus activos de información.

RRHH

Debe mantener constante capacitación y sensibilización a los trabajadores y colaboradores en cuanto al reporte de incidentes de seguridad de la información y vulnerabilidades de los sistemas de información. Debe hacer énfasis en:

a) Los riesgos de un control de seguridad ineficaz;

b) Qué es la violación de la integridad, confidencialidad o expectativas de disponibilidad de la información.

c) Los errores humanos.

d) Las no conformidades con políticas o directrices.

8.8.2 TIPOS DE INCIDENTES DE SEGURIDAD

- Adulteración del software.
- Saturación del sistema de información.
- Mal funcionamiento del software o equipo.
- Daño sobre activos de información.
- Caída o indisponibilidad de la plataforma o servicio.
- Intrusión o ataques internos o externos.
- Acceso no autorizado al sistema.
- Modificación no autorizada.
- Pérdida de información.
- Divulgación de información confidencial.
- Soborno por obtención de información o servicio no autorizado.
- Pérdida de licencia, registro de marca o permisos.
- Pérdida o robo de equipos.
- Interceptación de comunicaciones.
- Actos fraudulentos.

8.8.3 NIVELES DE CRITICIDAD, ESCALAMIENTO Y TIEMPOS DE RESPUESTA

El grupo responsable debe atender de manera inmediata el incidente de Seguridad de la Información, de acuerdo a los niveles de criticidad del evento / incidente a fin de darle el tratamiento adecuado.

Nivel	Criticidad	Escalamiento
Alto	Interrumpe seriamente la operación de la empresa, el incidente puede tener velocidad significativa/rápida en su propagación y ocasionar daños de activos. Podría llegar a afectar más de un tipo de activo.	Se escala a los proveedores pertinentes y si es el caso, a las autoridades externas competentes. El responsable de gestionar este tipo de incidente es el Jefe de Administración o de Sistemas.
Medio	Interrumpe en un periodo corto de tiempo los procesos generales de la empresa, el incidente/evento compromete un activo importante.	Se escala al Comité de Seguridad del SGSI, los responsables de gestionar este tipo de incidentes es Jefatura de Sistemas, Administrador de sistemas de la EC, Jefe de Soporte o Jefes de las áreas involucradas.
Bajo	No interrumpe los procesos generales de la empresa, el incidente/evento, se detecta y puede controlarse fácilmente con recursos existentes en la empresa.	Se escala al responsable del activo de información involucrado en caso de ser necesario.

Los tiempos de respuesta y de resolución también deben tomarse en cuenta por nivel de criticidad:

Nivel	Tiempo de respuesta	Tiempo de resolución
Alto	Dentro de 15 minutos	Dentro de 6 horas
Medio	Dentro de 30 minutos	Dentro de 12 horas
Bajo	Dentro de 8 horas	Dentro de 3 días hábiles

8.8.4 PROCEDIMIENTO

Actividades	Descripción	Responsable
Reportar el incidente de seguridad	Los trabajadores y colaboradores con acceso a información de la empresa nota que se está presentando un incidente a los activos de la empresa debe proceder a reportar esta situación como un evento o incidente de seguridad al líder inmediato o al grupo de su círculo correspondiente.	Trabajadores y colaboradores
Registrar evento o incidente	Se realiza el registro correspondiente en el formulario Log de incidencias de la aplicación yanapa.pe (SOPORTE > Crear Ticket INTERNO > Log de Incidencia) y se realiza el llenado: 1. Indicar el servicio o activo que ha sufrido el incidente. 2. Agregar en "Relacionado a" la opción de SGSI. 3. Redactar la descripción del incidente e incluir: 1. Tipo de incidente. 2. Los servicios, plataformas o dispositivos involucrados. 3. La fecha y hora exacta del incidente. 1. Se puede agregar archivos o evidencia que ayude a la solución del incidente. Evitar cualquier manipulación que pueda comprometer la integridad de la evidencia. La aplicación también puede detectar automáticamente los incidentes, registrarlos y hasta cerrarlos.	Trabajadores, colaboradores y LCs
Evaluar el impacto	Evaluar qué tipo de evento/incidente es el que se presenta, a qué otros activos puede estar afectando, cuál es alcance del mismo, qué pronóstico tiene de expansión, así como los daños potenciales o reales que se generen. Para evaluar la severidad de los eventos/incidentes se considerará la relevancia de los activos y el nivel del incidente.	Líder de Sistemas u Oficial de Seguridad
Identificar la relevancia del activo	De acuerdo a la verificación de los riesgos asociados a los activos de información que se encuentran en la Metodología De Análisis De Riesgos De Seguridad de la Información, se establecerá la afectación del activo de información; incluyendo, si es necesario, el valor económico y la cantidad de información relevante para la empresa contenida en el mismo.	Oficial de Seguridad o LCs
Identificar el nivel del incidente	Identificar el nivel de afectación del incidente de acuerdo a los Niveles de Criticidad del Evento/Incidente descritos en el presente documento.	Oficial de Seguridad o Líder de Sistemas

Escalar el incidente	Para buscar una solución al incidente tener en cuenta los niveles de escalamiento.	Oficial de Seguridad de la Información
Dar respuesta a la incidencia e Iniciar la estrategia de Contención	1. tomar el tique de log de incidencia y registrar un segundo detalle: 1. Ingresar la condición que puede ser: 1. INVESTIGANDO 2. IDENTIFICANDO 3. MONITOREANDO 4. RESUELTO 1. La fecha y hora exacta de la respuesta 2. Agregar un detalle público 3. Si es necesario agregar un detalle interno 4. Asignar Privado o Público, según debe hacerse de conocimiento. 5. Se puede agregar archivos o evidencia que ayude a la solución del incidente. Junto al área encargada de gestionar el incidente de seguridad, deben tener en cuenta los siguientes factores para la contención del incidente o evento: • Daño potencial de recursos a causa del incidente. • Preservación de la evidencia. • Tiempo y recursos necesarios para poner en práctica la estrategia. • Efectividad de la estrategia. • Duración de las medidas a tomar. • Criticidad de los sistemas afectados. • Características de los posibles atacantes. • Si el incidente es de conocimiento público. • Pérdida económica. • Posibles implicaciones legales.	Líder de Sistemas y Comité de Seguridad
Manejar la evidencia	Dar correcto manejo a los datos y evidencias recolectadas, los cuales deben ser almacenados para futuras investigaciones e implementación de controles preventivos o de mejoramiento en la plataforma interna. La evidencia debe ser almacenada e incluir como mínimo lo siguiente: • Si el incidente ocurre en un sistema informático, evitar la manipulación de archivos, registros de actividad o dispositivos de almacenamiento digital. • Fotografiar o grabar en video la disposición física de los dispositivos y el entorno inmediato. La información que debe ser custodiada por el Oficial de Seguridad de la Información incluye: • Cantidad de incidentes presentados y tratados. • Tiempo asignado a los incidentes. • Daños ocasionados. • Vulnerabilidades explotadas. • Cantidad de activos de información involucrados. • Pérdidas. El almacenamiento físico seguro de las evidencias (en caso sea necesario) estará custodiado por el Oficial de seguridad de la información.	Oficial de Seguridad y Comité de Seguridad de la Información
Identificar las fuentes de ataque	Identificar las posibles fuentes de ataque posteriormente mencionadas: • Empleados descontentos. • Baja concientización. • Falta de Previsión de Contingencias. • Falta de políticas.	Comité de Seguridad de la Información

	• Desastres Naturales. • Inadecuada protección de la Infraestructura. • Confianza creciente en los sistemas • Virus. • Robo de información confidencial. • Violación a la privacidad. • Denegación de Servicios. • Hacking.	
Establecer la estrategia de Erradicación	Tener en cuenta para definir/decidir las estrategias de erradicación los siguientes factores: •Tiempo y recursos necesarios para poner en práctica la estrategia. •Efectividad de la Estrategia. •Pérdida económica. •Posibles implicaciones legales. •Relación costo-beneficio de la estrategia. •Experiencias anteriores. •Identificación de Usuarios o servicios comprometidos para proceder a desactivarlos. Registrar la solución del incidente de seguridad si no ha sido resuelto en el registro de respuesta, agregar un detalle: 1. La condición será RESUELTO. 2) La fecha y hora exacta de la solución. 3) Agregar un detalle interno. 4) Si es necesario agregar un detalle público.	LCs, Oficial de de seguridad, comité de seguridad
Aplicar los procedimientos de Recuperación	Tener en cuenta si se deben aplicar procedimientos de recuperación.	Comité de Seguridad de la Información
Realizar el análisis Post-Incidentes	Garantizar el correcto manejo de las lecciones aprendidas, de la siguiente manera: • Utilizar el Log de Incidencia generado y agregar un detalle “lección”. • Periódicamente analizar los eventos e incidentes presentados durante el periodo. Se busca definir esquemas más efectivos para responder ante situaciones que afecten la seguridad de la información en la empresa. Entre las actividades que se realizan está: • Mantener la documentación de los eventos e incidentes de seguridad de la Información. • Integrar, de ser necesarios, los eventos e Incidentes a la Matriz de Riesgos de los Activos. • Realización de capacitaciones en lo relacionado a eventos e incidentes de seguridad de la información.	Comité de Seguridad de la Información

	• Analizar los hechos y tomar decisiones.	

8.9 SEGURIDAD EN REDES

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.

8.10 MONITOREO

Se definen en el punto numero 8.7 PLANIFICACIÓN DEL SISTEMA

8.11 INTERCAMBIO DE DATOS

Mediante el documento LN-MET-001 METODOLOGÍA DE GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN se evalúan las vulnerabilidades y riesgos de seguridad relacionados al intercambio de datos y software, y estos son manejados de manera apropiada de acuerdo a su impacto sobre las operaciones del SVA.

8.12 GESTIÓN DE ACCESOS

PLATAFORMA	CONTROL		PERSONAL	PERFIL/PERMISOS
HSM (SE y CP5)	Ingreso por medio del PROXMOX		Jefe de sistemas, Gerente, Sistemas	titulares (4) el acceso es de control dual
Servidor DELL POWEREDGE R430	Ingreso por medio de una bios usuario y contraseña		Jefe de sistemas, Gerente, Sistemas	Usuario administrador
PROXMOX	Ingreso por medio de 2 certificados digitales	configuración con el ip de la red	Titulares de las claves	Usuario administrador

8.12 DOCUMENTACIÓN

La información crítica y sensible, es gestionada y archivada en nuestro sistema propio de documentos llamado “YANAPA”, al ser digital es protegida contra daño ambiental o intencional, así como acceso de lectura y modificación no autorizados, esto mediante nuestra gestion de acceso por usuarios.

8.13 CONTROL DE CAMBIO

Se implementa procedimientos de control de cambios para poner en producción modificaciones o parches de emergencia de aplicaciones críticas de software del SVA, a fin de evitar posteriores fallas o incompatibilidad con otros sistemas.

8.13.1 ROLES QUE PARTICIPAN EN EL PROCESO

Solicitante:

Responsable de proponer modificaciones desde Yanapa.pe. Se encarga de completar un formulario detallado, que incluye la descripción del cambio, su prioridad y la evidencia que justifica la necesidad del cambio. Además, el solicitante asume un rol activo en el proceso, asegurando el seguimiento, y colaborando estrechamente con los equipos técnicos durante todo el ciclo de vida del cambio, hasta su implementación final.

Jefe de Sistemas:

Encargado principal de la gestión de cambios, evalúa la viabilidad y el impacto de las propuestas, autoriza la ejecución de los cambios y coordina su implementación, asegurando que se mantenga la estabilidad y funcionalidad del sistema.

Desarrolladores:

Encargados de ejecutar las modificaciones en el sistema, deben seguir las instrucciones del solicitante de cambio y realizar pruebas de aceptación en colaboración con los equipos de control de calidad para garantizar la eficacia y eficiencia del cambio.

Encargados de QA:

Responsables de verificar la implementación precisa de los cambios, llevan a cabo pruebas de aceptación minuciosas, verificar que se ejecuten correctamente las pruebas en producción y no comprometan la integridad del sistema.

Gerencia:

Responsable principal de aprobar/autorizar cambios en personal crítico en la organización.

8.13.2 NIVELES DE CELERIDAD Y RESOLUCIÓN

Nivel	Descripción	Tiempo de resolución
Alto	Los cambios de nivel alto tienen un impacto significativo en el sistema y deben implementarse lo antes posible. Tienen un plazo fijo impuesto por la SUNAT, Indecopi u otra autoridad. Algunos ejemplos de cambios de nivel alto son la actualización de la seguridad del sistema para cumplir con un nuevo requisito legal, nuevas formas de envíos, nuevos plazos, entre otros.	Fecha límite
Medio	Los cambios de nivel medio tienen un impacto parcial en el sistema. No son necesarios de forma urgente, pero deben implementarse en un plazo razonable. Estos cambios pueden mejorar el rendimiento, la funcionalidad o la facilidad de uso del sistema. Algunos ejemplos de cambios de nivel medio son la mejora del rendimiento del sistema o la implementación de nuevas herramientas de desarrollo.	Fecha límite flexible
Bajo	Los cambios de nivel bajo tienen un impacto mínimo en el sistema. No tienen prioridad alguna en el sistema, por lo que no es necesario que se implementen con urgencia. Estos cambios pueden mejorar la apariencia, la usabilidad o la funcionalidad del sistema. Algunos ejemplos de cambios de nivel bajo son la mejora de la apariencia del sistema o la corrección de un error menor.	No tiene fecha límite

8.13.3 ESTADOS DE TICKETS

Nivel	Descripción

En espera	El ticket se encuentra en este estado cuando el solicitante ha enviado una solicitud de cambio, pero aún no ha sido aprobado o desaprobado. El solicitante puede modificar o eliminar el ticket en este estado.
En proceso	El ticket se encuentra en este estado cuando ha sido aprobado y está siendo implementado por el equipo de desarrollo. El equipo de desarrollo puede modificar el ticket en este estado.
Cerrados	El ticket se encuentra en este estado cuando el cambio ha sido implementado y probado con éxito. El ticket no puede ser modificado o eliminado en este estado.
Rechazados	El ticket se encuentra en este estado cuando el cambio no se implementará previo análisis y respuesta indicando motivos del rechazo realizado por el desarrollador.
Cancelados	El ticket se encontraba en proceso de implementación, sin embargo no se destinará recursos a su finalización indicando motivos de la cancelación realizada.

Mas descripción en nuestro documento LN-PRO-021 PROCEDIMIENTO DE GESTIÓN DE CAMBIOS

9 TERMINO DE LA ORGANIZACIÓN

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 y/o TSA 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.

10 REGISTRO DE AUDITORIA

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.

LLAMA.PE almacena la información de los registros de auditoría al menos durante diez(10) años.

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.

11 ASPECTOS LEGALES

11.1 POLITICA DE REEMBOLSO

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.

11.2 COBERTURA DE SEGURO

El monto mínimo de la póliza es de $ 35 000. 00 dólares americanos.

11.3 INFORMACIÓN 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.

11.3.1 INFORMACIÓN NO CONFIDENCIAL

Se considera como información no confidencial toda información encontrada en nuestro repositorio https://repositorio.llama.pe/ y pagina web

11.4 DERECHOS DE PROPIEDAD INTELECTUAL

LLAMA.PE es titular de los derechos de propiedad intelectual, que puedan derivarse del sistema de certificación que regula esta DPFR 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.

11.5 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

11.5.1 NOTIFICACIONES Y COMUNICACIONES ENTRE PARTICIPANTES

Tipo de comunicación	Medio autorizado	Requisitos de seguridad
Notificaciones administrativas o legales	Correo electrónico institucional legal@lma.pe	Documento firmado
Comunicaciones operativas entre AC y ER	Sistema interno de gestión documental, plataforma PKI interna o canal cifrado TLS	Registro automático de transacciones
Comunicaciones con titular/suscriptores	Correo electrónico registrado en el proceso de emisión o portal de usuario hacia soporte@llama.pe o realizar un ticket en https://ayuda.llama.pe/ticket	Validación de correo del titular/suscriptor
Comunicaciones con terceros que confían	Publicaciones en el sitio web oficial de la AC o repositorio público de certificados y CRL	Acceso seguro HTTPS y sello de tiempo
Comunicaciones con la AAC (INDECOPI)	Oficio digital firmado electrónicamente o envío por sistema de trámite documentario oficial	Acuse de recibo electrónico

11.6 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 al Reglamento de la Ley de Certificados Digitales, y a la Ley de Firmas y Certificados Digitales – Ley 27269 y la resolución N° 175-2025/DGI-INDECOPI., para el reconocimiento legal de los servicios que brinda la EC de LLAMA.PE bajo las directrices definidas en el presente documento.

11.7 EXONERACIÓN DE RESPONSABILIDAD

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

- Estado de Guerra, desastres naturales o cualquier otro caso de Fuerza Mayor
- Por el uso de los certificados siempre y cuando exceda de lo dispuesto en la normativa vigente y la presente Política de Certificación
- Por el uso indebido o fraudulento de los certificados o CRL's emitidos por la Autoridad de Certificación
- Por el uso de la información contenida en el Certificado o en la CRL.
- 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.
- Por el perjuicio causado en el periodo de verificación de las causas de revocación /suspensión.
- Por el contenido de los mensajes o documentos firmados o cifrados digitalmente.
- Por la no recuperación de documentos cifrados con la clave pública del Suscriptor.
- Fraude en la documentación presentada por el solicitante.

12 FRECUENCIA DE PUBLICACIÓN

Con autorización del Responsable de la Entidad 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