# POLÍTICA DE SEGURIDAD ER

VERSIÓN: V2.3

PUBLICO

OFICIAL

PARA: LLAMA.PE

HISTORIAL DE VERSIONES

| VERSIÓN | DESCRIPCIÓN | REALIZADO POR | FECHA |
|---|---|---|---|
| V2.3 | 2.0: 20/06/18 Operador de registro Responsable de la EC Se especifican los actuales proveedores de la EC a lo largo del documento. Se agrega historial de versiones. 2.1: 05/06/19 Operador de registro Responsable de la EC Se removió del documento a ER y EC con los cuales ya no colaboramos. 2.2: 07/01/20 Operador de registro Responsable de la EC Se amplía el ámbito de aplicación a la TSA 2.3: 10/03/2021 CISO Responsable de la EC Actualización de documento y formato | JORGE ENRIQUE MIGUEL ZELAYARÁN SANCHEZ | 2022-12-26 |
| V1.0 | Actualización de documento y formato | LOUIE ALBERTO DIAZ MARTICORENA | 2022-04-25 |

# Tabla de contenido


- 1 INTRODUCCIÓN
- 2 OBJETIVO
- 3 OBJETO DE LA ACREDITACIÓN
- 4 DEFINICIONES
  - 4.1 DEFINICIONES
- 5 EVALUACIÓN DE RIESGOS
  - 5.1 CONDICIONES GENERALES
- 6 POLÍTICA DE CONTROL DE ACCESO
- 7 SEGURIDAD DEL PERSONAL
- 8 SEGURIDAD FISICA
- 9 SEGURIDAD DE COMUNICACIONES Y REDES
- 10 MANTENIMIENTO DE EQUIPOS Y SU DESECHO
- 11 CONTROL DE CAMBIOS Y CONFIGURACIÓN
- 12 PLANIFICACIÓN DE CONTINGENCIAS.
- 13 AUDITORÍAS Y DETECCIÓN DE INTRUSIONES.
- 14 MEDIOS DE ALMACENAMIENTO.

# POLÍTICA DE SEGURIDAD ER

## 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 basados en la nube para instituciones financieras, gobiernos, organizaciones de todo tipo y empresas que tienen que realizar comercio, las comunicaciones, entrega de contenido e interacciones con la comunidad digital de forma segura.

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

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

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

En calidad de Autoridad de Sellado de Tiempo, LLAMA.PE presta los servicios de sellado de tiempo siguiendo la regulación establecida por el marco de la IOFE.

## 2 OBJETIVO

Este documento 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 Entidad de Registro (ER) en el marco del cumplimiento de los requerimientos de las Guías de Acreditación establecidas por el INDECOPI.

## 3 OBJETO DE LA ACREDITACIÓN

El alcance de la acreditación cubre la infraestructura y los sistemas de LLAMA.PE en la entrega de sus servicios de certificación y sellado de tiempo.

## 4 DEFINICIONES

### 4.1 DEFINICIONES

- Entidad de Certificación – EC: Entidad que presta servicios de emisión, revocación y re-emisión de certificados digitales en el marco de la regulación establecida por la IOFE.
- Entidad de Registro – ER: Entidad que realiza los procesos de verificación de identidad de los solicitantes de los servicios de certificación digital y que se encarga de custodiar esta misma información.
- Autoridad de Sellado de Tiempo – TSA: Entidad que emite los sellos de tiempo, en los cuales confían los suscriptores y terceros que confían.
- Políticas y Prácticas: Conjunto de declaraciones y reglas que indican el marco de aplicabilidad de los servicios para una comunidad de usuarios definida y que comunica el cumplimiento legal y regulatorio de los titulares y suscriptores.
- Titular y/o suscriptor: Entidad que requiere los servicios provistos por la EC, ER o TSA, 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/o registrado con un sello de tiempo, y que confía en la validez de las transacciones realizadas.

## 5 EVALUACIÓN DE RIESGOS

Se identifica y valora los activos que corresponden a la ER. Identificación de amenazas y vulnerabilidades de los activos críticos. Evaluación del impacto de los riesgos. Tratamiento de los riesgos de impacto grave y moderado que puedan presentarse en los procesos de registro contemplados por la ER.

Una metodología de riesgo es una herramienta fundamental que permite identificar los riesgos y los requerimientos de los activos críticos que sostienen las operaciones del servicio de certificación digital y así priorizar la inversión de recursos en el tratamiento de riesgos y prevenir el impacto de incidentes negativos que puedan afectar significativamente este servicio, en este caso LLAMA.PE ha utilizado parte de la metodología MAGERIT junto con la propia metodología de la empresa.

### 5.1 CONDICIONES GENERALES

- El proceso de identificación, análisis y evaluación de riesgos de seguridad de la información se realizará una vez al año o cuando ocurran cambios en los activos y/o proceso que forma parte del alcance del SGSI, el cual se llevará a cabo por el CISO
- El proceso de tratamiento de riesgos de seguridad de la información se realiza posterior a la culminación del proceso de evaluación de riesgos de seguridad de la información.
- Para la definición del marco de trabajo del proceso de evaluación de riesgos de seguridad de la información el CISO de la Información convocará al Propietario del Riesgo y personal involucrado en los procesos parte del alcance del SGSI - que se considere.

LLAMA.PE cuenta con certificacion ISO 27001 y los documentos relacionados a la evaluación de riesgos son los siguientes:

- INVENTARIO DE ACTIVOS DE INFORMACIÓN (FIAI)
- METODOLOGÍA DE GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN (MGSI)
- MATRIZ DE RIESGO

## 6 POLÍTICA DE CONTROL DE ACCESO

A continuación se detallan los controles de acceso implementados para la protección de la información sensible, considerando el acceso a equipos informáticos, software, lectura y escritura de documentos tanto físicos como electrónicos. Asimismo se deben considerar los controles de acceso a los ambientes donde se encuentra la información sensible. Todos los controles implementados están basados en los resultados de la evaluación de riesgos.

Se establece que el personal de Llama.pe y terceros deben acogerse a los controles de seguridad establecidos, tomando en cuenta los puntos siguientes:

- El Administrador de Sistemas será el encargado de hacer la gestión con el Oficial de Seguridad de la Información a fin de otorgar el acceso a los sistemas de información y servicios a los empleados y terceros, esto por requerimiento del jefe del área donde labora el empleado o tercero.
- Los sistemas de información de Llama.pe ("YANAPA") deben proveer la gestión y administración de los usuarios (internos, externos), crear, editar e inactivar perfiles de acuerdo a lo requerido para el desarrollo de sus funciones. Así mismo los privilegios que tienen dentro de los mismos.
- Para el acceso a los sistemas de información, los usuarios deben hacer buen uso de sus claves de acceso asignadas que serán gestionadas en AWS por el Gerente general y el Administrador de Sistema
- Para el acceso a lugares externos donde Llama.pe tenga almacenado equipos o información (LUMEN) solo se tendrá acceso mediante una lista firmada por el representante legal de la empresa y en esa lista solo estarán los miembros del SGSI y los auditores de ser necesario.

LLAMA.PE cuenta con certificacion ISO 27001 y los documentos relacionados al control de accesos son los siguiente:

- POLÍTICA DE CONTROL DE ACCESOS (PCA)
- PROCEDIMIENTO DE CONTROL DE ACCESO AL CÓDIGO FUENTE (PCACF)
- PROCEDIMIENTO DE GESTIÓN DE LOS DERECHOS DE ACCESO PRIVILEGIADOS (PGDAP)
- PROCEDIMIENTO DE RESTRICCIONES DE ACCESO A LA INFORMACIÓN (PRAI)

## 7 SEGURIDAD DEL PERSONAL

Llama.pe debe mantener un perímetro de seguridad para proteger las áreas que contienen la información, teniendo en cuenta los niveles de clasificación y ubicación, para lo cual debe realizar asignación de los responsables de los activos de información.

- El ingresa a la oficina principal son controlados por recepcionista.
- El personal de Llama.pe solo debe ingresar a aquellas áreas donde se encuentre autorizado.
- Existen implementos de seguridad contra amenazas físicas (incendios, inundaciones; etc) extintores; etc.
- Se emplea infraestructura de cajas xxxxx para almacenar documentos con información confidencial.
- Se emplea infraestructura virtual para almacenar los activos de información en formato digital.

Llama.pe aplica protección física contra los daños que puedan ocurrir por fuego, inundación, terremotos, disturbios y otros causados por el hombre.

Se debe considerar los siguientes lineamientos para evitar los daños por incidentes mencionados:

- Debe certificarse la existencia de protección contra terremotos e incendios.
- El equipo de reemplazo debe ubicarse a una distancia segura para evitar el daño de un desastre que afecte el local principal.
- Se debe proporcionar equipo contra incendios ubicado adecuadamente.
- Contar con respaldo de toda la información alojada en la nube esto a fin de asegurar que esta no se pierda en caso ocurra un desastre natural de gran envergadura.

Se describen los métodos de verificación de datos y antecedentes, así como los perfiles considerados para la selección tanto del personal que ocupa roles de confianza, incluyendo al Responsable de Seguridad. Se detallan las responsabilidades del personal, así como los medios y mecanismos de comunicación y capacitación.

LLAMA.PE cuenta con certificacion ISO 27001 y los documentos relacionados a la seguridad del personal son los siguiente:

- MANUAL DE ORGANIZACIÓN Y FUNCIONES (MOF)
- PROCEDIMIENTO DE EVALUACIÓN DE PERSONAL (PEP)

# 8 SEGURIDAD FISICA

Se describen los elementos que integran la seguridad física tales como alarmas de seguridad física, cerco perimetral, guardias, eliminación de material en desuso, llaves, etc. Descripción de los procedimientos para asegurar la seguridad física y ambiental.

Llama.pe aplica protección física contra los daños que puedan ocurrir por fuego, inundación, terremotos, disturbios y otros causados por el hombre.

Se debe considerar los siguientes lineamientos para evitar los daños por incidentes mencionados:

- Debe certificarse la existencia de protección contra terremotos e incendios.
- El equipo de reemplazo debe ubicarse a una distancia segura para evitar el daño de un desastre que afecte el local principal.
- Se debe proporcionar equipo contra incendios ubicado adecuadamente.
- Contar con respaldo de toda la información alojada en la nube esto a fin de asegurar que esta no se pierda en caso ocurra un desastre natural de gran envergadura.

LLAMA.PE cuenta con certificacion ISO 27001 y los documentos relacionados a la seguridad física son los siguiente:

- POLÍTICA DE SEGURIDAD FÍSICA Y AMBIENTAL (PSFA) A.11

# 9 SEGURIDAD DE COMUNICACIONES Y REDES

Se describen las medidas de seguridad en el tema de comunicaciones y redes tanto a nivel interno como a nivel externo. También se establecen los requerimientos de seguridad que deben cumplirse cuando existe una relación con otros medios de comunicación.

El Administrador del Sistema y el Jefe de sistemas garantizan la seguridad de los datos y los servicios conectados en las redes de la empresa, contra el acceso no autorizado y deben considerar los siguientes lineamientos:

- Establecer controles para salvaguardar la confidencialidad, integridad y disponibilidad del procesamiento de los datos que pasan a través de redes públicas y para proteger los sistemas conectados (Solo autorizar las IP que se encuentran debidamente registradas en la plataforma).
- Establecer acuerdos con el proveedor del servicio de red de tal forma que siempre exista disponibilidad del servicio

La Jefatura de Sistemas implementará dichos controles

LLAMA.PE cuenta con certificacion ISO 27001 y los documentos relacionados a la seguridad de comunicaciones y redes son los siguiente:

- POLÍTICA DE SEGURIDAD EN LAS TELECOMUNICACIONES (PST)
- PROCEDIMIENTOS DE CONTROL DE RED (PCR)
- ACUERDO DE CONFIDENCIALIDAD PARA TERCEROS (ACT)

# 10 MANTENIMIENTO DE EQUIPOS Y SU DESECHO

Se describen las normas y procedimientos que aseguran la correcta utilización de los equipos informáticos así como su mantenimiento. También se detallan las normas y procedimientos cuando el equipo es reemplazado, decomisado, manipulado, desechado (hardware y software). Descripción del tipo de personal que está autorizado para el mantenimiento del equipo. LLAMA.PE cuenta con certificacion ISO 27001 y los documentos relacionados al mantenimiento de equipos son los siguiente:

- POLÍTICA DE SEGURIDAD FÍSICA Y AMBIENTAL (PSFA) A.11
- PROCEDIMIENTOS DE DISPOSICIÓN O REUTILIZACIÓN SEGURA DE EQUIPOS (PDRSE)
- PROCEDIMIENTO DE EQUIPO DE USUARIO DESATENDIDO
- FORMATO DE BAJA DE EQUIPO

# 11 CONTROL DE CAMBIOS Y CONFIGURACIÓN

Se establecen los responsables que tienen autorización para la aprobación de cambios a los sistemas. Se detallan los procesos de aprobación de cambios a los sistemas.

1. El colaborador debe de ingresar a https://yanapa.pe/ logeándose con su correo corporativo.
2. Dirigirse a la sección “Tickets/reclamos” e ingresar a “Gestionar Tickets”. Luego hacer clic en “Solicitud de Cambio”
3. Llenar todos los campos del formulario y enviarlo.
4. Se enviará un mensaje de correo al Jefe de Sistemas y Administrador de sistema para que revisen la solicitud de cambio.
5. Los cambios aceptados deben ser aprobados de acuerdo con su clasificación y nivel de impacto, por el Gerente o Responsable de la ER,EC, TSA Y SDF.
6. Cuando la solicitud de cambio es debidamente autorizada su implementación es planeada, comunicada y ejecutada.

Se implementa para incorporar seguridad a los sistemas de información (propios) y a las mejoras o actualizaciones que se les incorporen.

Los requerimientos para nuevos sistemas o mejoras a los existentes especificarán la necesidad de controles. Estas especificaciones deben considerar los controles automáticos a incorporar al sistema.

Se debe tener en cuenta los siguientes lineamientos:

- Definir una guía de configuración de seguridad en el desarrollo del software, para que, durante las etapas de análisis y diseño del sistema, se incorporen a los requerimientos, los correspondientes controles de seguridad.
- Evaluar los requerimientos de seguridad y los controles requeridos, teniendo en cuenta que éstos deben ser proporcionales en costo y esfuerzo al valor del bien que se quiere proteger y al daño potencial que pudiera ocasionar a las actividades realizadas.
- Considerar que los controles introducidos en la etapa de diseño, son significativamente menos costosos de implementar y mantener que aquellos incluidos durante o después de la implementación.

LLAMA.PE cuenta con certificacion ISO 27001 y los documentos relacionados el control de cambios y configuración son los siguiente:

- POLÍTICA DE SEGURIDAD EN LAS OPERACIONES (PSO) A.12
- PROCEDIMIENTOS DE GESTIÓN DE CAMBIOS
- POLÍTICA DE ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMA DE INFORMACIÓN (PADMSI)

# 12 PLANIFICACIÓN DE CONTINGENCIAS.

Se describe la relación entre la valoración de riesgos y las acciones que se deben tomar como contingencia. LLAMA.PE cuenta con certificacion ISO 27001 y los documentos relacionados con la planificación de contingencias son los siguiente:

- INVENTARIO DE ACTIVOS DE INFORMACIÓN (FIAI)
- METODOLOGÍA DE GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN (MGSI)
- MATRIZ DE RIESGO
- POLÍTICA DE GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN (PGISI)

# 13 AUDITORÍAS Y DETECCIÓN DE INTRUSIONES.

Se establecen los objetivos de las auditorías. Su frecuencia y sistemas implicados. LLAMA.PE cuenta con certificacion ISO 27001 y los documentos relacionados las auditorias son los siguiente:

- PROCEDIMIENTO DE AUDITORÍAS INTERNAS (PAI)
- FORMATO DE AUDITORÍA INTERNA

# 14 MEDIOS DE ALMACENAMIENTO.

Se detallan todos los procedimientos de los medios de almacenamiento para asegurar la información, tales como respaldo y recuperación. LLAMA.PE cuenta con certificacion ISO 27001 y los documentos relacionados los medios de almacenamientos son los siguiente:

- POLÍTICA DE SEGURIDAD FÍSICA Y AMBIENTAL (PSFA) A.11
- POLÍTICA DE GESTIÓN DE ACTIVOS (PGA) A.8