llama.pe

POLÍTICA DE SEGURIDAD EC

VERSIÓN: V2.3

PUBLICO

OFICIAL

PARA: LLAMA.PE

HISTORIAL DE VERSIONES

VERSIÓN	DESCRIPCIÓN	REALIZADO POR	FECHA
V2.3	1.0 28/06/17 Operador de registro Responsable de la EC Versión inicial 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 10/03/22 CISO Responsable de la EC Actualización de formatos	LOUIE ALBERTO DIAZ MARTICORENA	2022-12-27

Tabla de contenido

POLÍTICA DE SEGURIDAD EC

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 Certificación (EC) y la Autoridad de Sellado de Tiempo (TSA); en el marco del cumplimiento de los requerimientos de las Guías de Acreditación establecidas por el INDECOPI. Debido a que la EC y TSA pertenecen a la misma infraestructura y que las operaciones de la TSA replican a las de la EC; dichos servicios comparten las mismas prácticas de seguridad de la información. En ese sentido, cada vez que el presente documento mencione la EC, se entenderá que también hace referencia a la TSA.

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 Y ABREVIACIONES

4.1 ABREVIACIONES

AAC: Autoridad Administrativa Competente

DN: (Distingued Name) Nombre Distintivo

EC: Entidad de Certificación

ER: Entidad de Registro

TSA: Autoridad de Sellado de Tiempo

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 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 RESPONSABILIDADES

Las responsabilidades contractuales, garantías financieras y coberturas de seguros son brindadas por LLAMA.PE de acuerdo con sus prácticas de certificación, registro y valor añadido, publicadas en:

https://llama.pe/repository

Las peticiones, quejas o reclamos para la atención de suscriptores y terceros debido a consultas relacionadas con el servicio que dispone la EC, ER y TSA; son recibidas directamente por LLAMA.PE mediante la línea telefónica o correo electrónico. Asimismo, pueden acercarse hacia las oficinas de LLAMA.PE, indicando que presenta una queja, reclamo o petición.

Datos de la EC, ER y TSA:

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/

6 CONTROLES FÍSICOS DE LA INSTALACIÓN, GESTIÓN Y OP.

6.1 CONTROLES FÍSICOS DE LA INFRAESTRUCTURA TECNOLÓGICA

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

6.1.1 UBICACIÓN FÍSICA Y CONSTRUCCIÓN

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

La infraestructura de las instalaciones subcontratadas está basada en el modelo de ingeniería "N+1".

Utilizando este modelo, los ingenieros determinan la capacidad total requerida para un elemento específico de infraestructura (ancho de banda, alimentación, aire acondicionado, etc.) Este requerimiento por capacidad es luego distribuido en "N+1" (ó "n + múltiples") componentes de infraestructura (líneas de telecomunicaciones, routers, sistemas de UPS, manejadores de aire, etc.), siendo suficientes "N" componentes para satisfacer los requerimientos de demanda máxima.

Asimismo, asegura que la infraestructura tecnológica será escalable de acuerdo con el crecimiento del volumen de los aplicativos de sus clientes.

El edificio fue diseñado, supervisado y construido para cumplir con lo dispuesto en el Reglamento Nacional de Edificaciones para un edificio de Telecomunicaciones y en especial a las Normas Técnicas de Edificación E.030 para Diseño Sismo Resistente y con la norma E.060 para Concreto Armado.

Los pisos de las instalaciones son losas macizas de concreto armado, con doble malla de fierro y con un espesor de 20 cm, con una resistencia de 1,000 Kg/m2a la sobrecarga, mientras que la sala de UPS y Baterías cuenta con 25cm de espesor y una resistencia de sobrecarga de 3,000 Kg/m2.

Los gabinetes se aseguran a la losa de concreto a través de cuatro (04) varillas roscadas de ½" de acero cincado de 90cm de longitud, con la finalidad de asegurarlos en su lugar en el caso de un sismo.

6.1.2 ACCESO FÍSICO

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

El monitoreo de estos sistemas lo realiza el operador del Centro de Control. El puesto de Operador se cubre todo el año durante las 24 horas del día.

El Centro de Control es el encargado de la administración de las credenciales, previa solicitud vía correo electrónico del gerente de un área específica.

En cuanto al sistema de control de accesos, si una persona a la cual se le ha asignado una tarjeta de proximidad con permisos de accesos específicos intenta ingresar a un área que no tiene permiso, se producirá una alarma visual y audible en la pantalla del sistema, observándose la ubicación de la puerta y la persona que intentó pasar por esa puerta. A continuación, el operador se comunicará con el agente de ronda para que acuda al punto a verificar qué es lo que ocurrió.

En cuanto al sistema de control de accesos a los diferentes ambientes de las instalaciones, se realiza a través de un software especializado, registra la data de los ingresos y salidas de las puertas de acceso a las instalaciones. Luego, el operador de Centro de Control puede efectuar previa autorización, el reporte de accesos de una persona específica.

En cuanto a la seguridad de acceso lógico, las instalaciones mantienen un segmento de Red totalmente independiente para la solución del cliente, también cuenta con esquemas que permiten la verificación, actualización y ejecución de procedimientos para evitar accesos no autorizados a los segmentos de red dedicados a los clientes. Por último, cuenta con servicios de autenticación para el acceso de los usuarios a la red mediante el cual se otorgan los permisos a la lista del personal autorizado por el cliente para utilizar el servicio.

La seguridad e integridad son mantenidas por un sistema de vigilancia vía circuito cerrado de televisión digital, alarmas de movimiento y personal las 24 horas del día.

El edificio cuenta con un sistema conformado por más de 50 cámaras de seguridad, entre fijas y de domos, distribuidas tanto en el edificio administrativo como en el Data Center. Las cámaras permiten supervisar los corredores de acceso hacia sus gabinetes, e identificar cualquier acceso hacia los mismos, pero en ningún momento estará apuntando directamente a los gabinetes, lo que asegura la confidencialidad del trabajo a ser realizado por personal del cliente o personal autorizado por éste.

Las cintas de las cámaras de video se almacenan hasta por un máximo de noventa (90) días calendario. De producirse algún incidente se puede solicitar el acceso a las cintas.

6.1.3 ALIMENTACIÓN ELÉCTRICA Y AIRE ACONDICIONADO

Las instalaciones subcontratadas por LLAMA.PE cuenta con una sala de generadores de energía totalmente independiente, ubicada en el sótano del área de servicios generales, a 12 metros de profundidad y a 20 metros de distancia del edificio.

El edificio total de la sala de generadores es de 300m2, incluyendo un tanque de 5,000 galones de Diesel 2, que, junto con los dos tanques de 500 galones, que están soterrados, suman 6,000 galones de este combustible. El acceso es con cerradura electrónica, cuenta con una barra anti-pánico al interior.

En cuanto al Sistema de Monitoreo para el Control de Equipos Eléctricos se hace a través del sistema SCADA, registra los siguientes componentes: Energía comercial, Transformadores y Grupos Electrógenos. Asimismo, los principales parámetros que se monitorean, en las tres fases, son: Voltaje, Amperaje, Kilowatt Hora, KW-R, Frecuencia.

Respecto de la Redundancia UPSs, en la sala de UPS y Baterías, se cuenta con un sistema múltiple de UPS. En caso de que uno falle, el resto puede adquirir la carga sin exceder su capacidad nominal. Las baterías de los UPS son cargadas por la red pública de energía eléctrica o por los generadores redundantes de reserva.

Por otro lado, las cargas eléctricas críticas son alimentadas por sistemas paralelos, redundantes de UPS, que se configuran con puente estático automático y con circuitos de derivación manuales. El tiempo de duración de la batería de cada UPS es suficiente teniendo en cuenta que para la entrada en régimen de los generadores diesel se requiere 1 minuto para su estabilización.

La capacidad de los UPS que forman parte de las soluciones para los clientes dependerá del consumo real y del consumo contratado. Se puede trabajar indistintamente con equipos con capacidad nominal de 120 KVA, 280KVA, 320 KVA o mayores. Estos UPS son compartidos y no a dedicación exclusiva.

El programa de mantenimiento de los UPS es semestral. Se miden y prueban los equipos y se realiza una limpieza, reparación o cambio de ser necesario. El programa de mantenimiento también se realiza bajo la filosofía N+1.

En cuanto a la autonomía del servicio de UPSs, cada módulo de UPS tiene su propia batería, con capacidad suficiente para sostener la red eléctrica por períodos de 30 minutos, en este caso el UPS solo debe trabajar hasta un máximo del 50% de su capacidad total, ya que en los sistemas paralelos los UPS comparten carga y en caso de falla de uno de ellos, el otro equipo asume la carga total. En la actualidad cada UPS está al 40%, en caso de que uno falle el otro llega al 80%.

Con relación al Sistema Automatizado La instalación subcontratada por Llama.pe, cuenta con dos tableros de transferencia automática TTA, y en cuanto la frecuencia de mantenimiento, es semestral.

Referente a la Redundancia en Generador de Energía, se disponen de dos turbogeneradores diesel de marca Caterpillar, en configuración 1+1, capaces de ponerse en marcha y acoplarse automáticamente a la red eléctrica en menos de 1 minuto.

El sistema de administración redundante de la energía eléctrica provee a todos los clientes y sistemas críticos potencia limpia e independiente. Este sistema fue diseñado para satisfacer como mínimo una potencia de 1.5 KVA/m de espacio sin considerar los equipos de aire acondicionado.

Es importante mencionar que se cumplen con los estándares de conexión a tierra especificados y recomendados por las normas ITU-T K-27 y ETS1.
En cuanto a la frecuencia de mantenimientos, los programas para los equipos son de dos tipos: el mantenimiento anual, que consiste en el cambio de aceite, petróleo, filtros, y encendido con carga, y el segundo, mantenimiento mensual, donde los equipos son prendidos en vacío y se verifican los principales parámetros de funcionamiento.

En consideración al aire acondicionado, la instalación subcontratada por LLAMA.PE dispone de múltiples unidades de precisión que aseguran una adecuada disipación de calor. En el caso de que la unidad de aire acondicionado falle, las otras unidades están diseñadas para satisfacer la carga térmica completa a los equipos albergados. Asimismo, está construido contemplando un piso elevado, a través del cual se provee aire climatizado a los racks de equipos.

En cuanto a las Unidades de Climatización, éstas son alimentadas tanto por la red eléctrica pública como por sistemas eléctricos de emergencia. Estas unidades están siendo constantemente monitoreadas por el sistema de control del edificio y una falla en cualquiera de sus componentes acciona inmediatamente una alarma. Presenta una capacidad de 15 toneladas de BTU por hora por cada unidad de climatización .

La temperatura en las instalaciones subcontratadas por Llama.pe es mantenida en 21° C +/- 3°C. Cada unidad de climatización, además controla la humedad relativa para mantenerla siempre en 40%, +/- 10%, evitando de esa forma la condensación del vapor de agua ambiental.

El programa de mantenimiento para los equipos de aire acondicionado es cada dos meses y está basado en el protocolo NSPA 75. Se utiliza un proceso de verificación permanente de la composición de aire en la sala de equipamiento, donde también se detectan presencia de humo, filtros de polvo, diferencia de temperatura, entre otros.

6.1.4 EXPOSICIÓN AL AGUA

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

6.1.5 PREVENCIÓN Y PROTECCIÓN DE INCENDIOS

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

Las puertas contrafuego se encuentran instaladas en las salidas de escape de ambas escaleras en todos los niveles del Edificio Administrativo y Edificio Técnico. La instalación también incluye los accesorios que sirven como complemento tales como barras antipánico, brazos cierras puertas y las bisagras cortafuego. Adjuntamos certificado de garantía de nuestras puertas que han sido sometidas a pruebas durante 90 minutos de exposición al fuego a más de 975°C.

Las instalaciones cuentan con dos tipos de piso técnico: Paneles de acero AS-1500 de 24” y paneles perforados PERF 1250 de 24”. Ambos paneles han sido elaborados con material no combustibles y tiene una Categoría A respecto del factor Retardo en Propagación de Fuego.

Las salas donde se albergan equipos informáticos disponen de sistemas de la supresión del fuego, que fue diseñado alrededor de un sistema de detección temprana, a través de un avanzado sistema analizador que detecta el humo en las primeras etapas de la combustión, por medio de un analizador de gases que inspecciona la composición del aire dentro de los ambientes. Este sistema de detección está además respaldado por sistemas iónicos de detección de partículas.

Asimismo, cuentan con un sistema de detección de humo con sensores fotoeléctricos y de extinción de incendios con agua, haciendo uso de rociadores o sprinklers. El sistema cumple con la norma internacional NFPA 25. El sistema de rociadores mantiene una presión de drenaje de 130 psi con válvula de drenaje cerrada y mantiene una presión de 120 psi con válvula de drenaje abierta. La inspección del Sistema es semestral.

En caso de accionarse un sistema de detección de incendio, el centro cuenta con un sistema de extinción redundante contra incendios por utilización de Gas FM-200. El mecanismo de extinción de incendios del agente FM-200 es activo. Su acción primaria es la de enfriar físicamente el incendio a nivel molecular. El agente FM-200 (HFC-227) pertenece al mismo tipo de compuestos que se usan en refrigeración, y como tal es un agente de transferencia de calor eficiente.

El FM-200 extrae literalmente la energía calorífica del incendio hasta el punto en que la reacción de combustión no puede mantenerse. Además, existe una acción de extinción química atribuible al agente FM-200. Durante un incendio se liberan pequeñas cantidades de radicales libres que inhiben la reacción en la cadena de combustión. Estos componentes no afectan a los equipos existentes en la sala. La descarga de FM-200 se realiza en un tiempo menor a los 10 segundos, y no afecta el equipamiento eléctrico.

6.1.6 SEGURIDAD DE EQUIPOS

Se cuenta con un Procedimiento de Seguridad física y del equipo que asegura la disponibilidad e integridad de los equipos con los que cuenta LLAMA.PE.

6.1.7 SISTEMA DE ALMACENAMIENTO

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

6.1.8 ELIMINACIÓN DEL MATERIAL DE ALMACENAMIENTO DE LA INFORMACIÓN

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

En particular, para la información contenida en discos duros regulables se borrará el contenido y se escribirán ceros a bajo nivel.

6.1.9 BACKUP FUERA DE LA INSTALACIÓN

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

6.2 CONTROLES DE PROCEDIMIENTO

6.2.1 ROLES DE CONFIANZA

LLAMA.PE, garantiza que todo el personal de confianza es el descrito en el documento Diagrama Organizacional 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 asignados para LLAMA.PE son los siguientes:

- Administrador del sistema operativo: Encargado de instalar y configurar el sistema operativo para la aplicación de la EC (EJBCA); establecer las cuentas de usuario y credenciales en los sistemas anteriores; y controlar el acceso de administración a los sistemas anteriores.
- Administrador de la aplicación: Encargado de instalar y configurar la aplicación de la EC (EJBCA) de acuerdo al procedimiento establecido; y establecer cuentas de usuarios en la aplicación de la EC (EJBCA).
- Custodio de los materiales criptográficos: Responsable de mantener un inventario preciso de todos los dispositivos involucrados; vigilar que ninguno de los dispositivos sea reemplazado durante la ejecución del procedimiento; asegurarse de que el servidor y el HSM sean apropiadamente trasladados a su ubicación definitiva en el centro de datos después de completado el procedimiento; asegurarse de que el PIN pad sea almacenado de manera segura; asegurarse de que las tarjetas inteligentes se encuentren debidamente protegidas después de completado el procedimiento; almacenar el token utilizado para la autenticación como superadministrador ante la aplicación de la EC (EJBCA).
- Auditor de Sistemas de la EC: Responsable del cumplimiento de los procedimientos operativos. Es una persona externa al departamento de Sistemas de Información.
- Auditor de Sistemas de la ER: Responsable de auditar los logs del sistema de registro de LLAMA.PE.
- Administrador de Sistemas de la ER: Encargado de instalar y configurar el sistema de registro de LLAMA.PE. Además de dar de alta o baja a los ORs.
- Operador de Registro: Encargado de realizar operaciones diarias como aprobar las solicitudes de emisión, revocación y re-emisión de certificados digitales.
- Oficial de Seguridad y Privacidad: Encargado de coordinar, controlar y hacer cumplir las medidas de seguridad definidas por la Política de seguridad y de privacidad de LLAMA.PE. Debe encargarse aspecto relacionado con la seguridad de la información: lógica, física, redes, organizativa, etc. Además de la privacidad y protección de datos personales.
- Comité de Seguridad: Es un comité conformado por el Responsable de la EC, ER y TSA, y el Administrador de Sistemas de la EC, que se encarga de la evaluación y toma de decisiones en cuanto a la gestión de la seguridad de información. Periódicamente, el Oficial de Seguridad informa a dicho comité sobre vulnerabilidades detectadas, incidentes de seguridad, entre otros.

6.2.2 NÚMERO DE PERSONAS REQUERIDAS POR TAREA

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

6.2.3 IDENTIFICACIÓN Y AUTENTICACIÓN PARA CADA ROL

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

6.3 CONTROLES DE PERSONAL

6.3.1 REQUISITOS SOBRE LA CUALIFICACIÓN, EXPERIENCIA Y CONOCIMIENTO PROFESIONALES

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

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.

6.3.2 PROCEDIMIENTO DE COMPROBACIÓN DE ANTECEDENTES

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

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

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

6.3.3 REQUISITOS DE FORMACIÓN

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

El plan de formación incluye los siguientes contenidos:

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

6.3.4 REQUISITOS Y FRECUENCIA DE ACTUALIZACIÓN DE FORMACIÓN

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

6.3.5 FRECUENCIA Y SECUENCIA DE ROTACIÓN DE TAREAS

No estipulado.

6.3.6 SANCIONES POR ACTUACIONES NO AUTORIZADAS

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

6.3.7 REQUISITOS DE CONTRATACIÓN DE TERCEROS

Los empleados contratados para realizar tareas confiables firman anteriormente las cláusulas de confidencialidad y los requerimientos operacionales empleados por LLAMA.PE. Cualquier acción que comprometa la seguridad de los procesos aceptados 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, o en otras partes de la CPS, serán aplicados y cumplidos por el tercero que realice las funciones de operación de los servicios de certificación, la entidad de certificación será responsable en todo caso de la efectiva ejecución. Estos aspectos quedan concretados en el instrumento jurídico utilizado para acordar la prestación de los servicios de certificación por tercero distinto de LLAMA.PE debiendo obligarse los terceros a cumplir con los requerimientos exigidos por LLAMA.PE.

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.

6.3.8 DOCUMENTACIÓN PROPORCIONADA AL PERSONAL

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

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.

6.4 PROCEDIMIENTOS DE CONTROL DE SEGURIDAD

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

6.4.1 TIPOS DE EVENTOS REGISTRADOS

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

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 archivos.
- 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 de este.

Mensualmente o cada vez que se produce una alerta de seguridad, el Administrador de Sistemas de LLAMA.PE se encarga de revisar los registros de auditoría.

El procesamiento de los registros de auditoría consiste en una revisión de los registros que incluye la verificación de que éstos no han sido manipulados, una breve inspección de todas las entradas de registro y una investigación más profunda de cualquier alerta o irregularidad en los registros.

Se mantiene un sistema que permite garantizar que la información que se guarda incluye como mínimo la fecha y la hora del evento.

6.4.2 PERIODO DE RETENCIÓN DE LOS REGISTROS DE AUDITORÍA

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

6.4.3 PROTECCIÓN DE LOS REGISTROS DE AUDITORÍA

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

6.4.4 PROCEDIMIENTOS DE BACKUP DE LOS REGISTROS DE AUDITORÍA

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

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

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

6.4.6 NOTIFICACIÓN AL SUJETO CAUSA DEL EVENTO

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

6.4.7 ANÁLISIS DE VULNERABILIDADES

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

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

6.5 ARCHIVO DE REGISTROS

6.5.1 TIPOS DE EVENTOS ARCHIVADOS

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

- Todos los datos relativos a los certificados, incluyendo los contratos de suscriptor/titular.
- Los datos relativos a su identificación.
- Solicitudes de emisión y revocación de certificados.
- Estado de acreditación.
- Tipo de documento presentado en la solicitud del certificado.
- Número de identificación único proporcionado por el documento anterior.
- Todos los certificados emitidos o publicados.
- Claves públicas de la EC.
- El registro de auditorías.

- Políticas y Prácticas de Certificación.

LLAMA.PE responsable del correcto archivo de todo este material.

6.5.2 PERIODO DE CONSERVACIÓN

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

6.5.3 PROTECCIÓN DE ARCHIVOS

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

6.5.4 PROCEDIMIENTOS DE BACKUP DEL ARCHIVO DE REGISTROS

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

6.5.5 REQUISITOS PARA EL SELLADO DE TIEMPO DE LOS REGISTROS

No aplica.

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

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

6.5.7 PROCEDIMIENTOS PARA OBTENER Y VERIFICAR INFORMACIÓN ARCHIVADA.

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

6.6 CAMBIO DE CLAVES DE UNA EC

El cambio de claves de entidad final es realizado mediante la realización de un nuevo proceso de emisión (ver apartado correspondiente de las prácticas de EC y TSA).

En EC (EC Raíz, EC Subordinada) y TSA, antes de que el certificado caduque, se realizará un cambio de claves. El certificado a actualizar de la EC y su clave privada sólo se usará para la firma de CRLs mientras existan certificados activos emitidos por dicha EC.

Se generará un nuevo certificado de EC con una clave privada nueva y un CN (common name) distinto al del certificado de la EC a sustituir.

También se realizará cambio de certificado de una EC cuando el estado del arte criptográfico (algoritmos, tamaño de claves) lo requiera.

6.7 RECUPERACIÓN EN CASO DE COMPROMISO Y DESASTRE

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

Una recuperación de la efectividad de las claves en términos de negocio dependerá principalmente de la duración de estos procesos de reconocimiento. El Plan de continuidad incorpora estos términos puramente técnicos y operativos para que las nuevas claves estén disponibles, pero no así su reconocimiento por terceros.

El compromiso de los algoritmos o los parámetros asociados utilizados en la generación de certificados digitales o servicios asociados se incorporan también en el Plan de continuidad.

Cualquier fallo en la consecución de las metas marcadas por este Plan de continuidad, será tratado como razonablemente inevitable a no ser que dicho fallo se deba a un incumplimiento de las obligaciones de LLAMA.PE para implementar dichos procesos.

El Plan de continuidad de LLAMA.PE trata el compromiso de la clave privada de la EC como una situación de desastre.

En caso de compromiso de una clave raíz:

- Informará a todos los suscriptores, titulares y otras ECs con los cuales tenga acuerdos u otro tipo de relación del compromiso.
- Indicará que los certificados e información relativa al estado de la revocación firmados usando esta clave no son válidos.

Asimismo, se han desarrollado Planes de Recuperación (DRP) en caso de compromiso de las claves de la EC, en caso de cese de trabajo de personal de confianza y, además, se elaborarán más DRPs conforme se detecten situaciones donde se podría vulnerar la seguridad de la EC. El Responsable de la EC y el Oficial de Seguridad serán los principales responsables de realizar las DRPs; sin embargo, en cada uno se indicará si hay más roles relacionados a las pruebas.

6.8 CESE DE UNA EC O ER

6.8.1 CESE DE LA EC DE LLAMA.PE

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

- Proveerá de los fondos necesarios, mediante carta fianza, para continuar la finalización de las actividades de revocación.
- Informará a los suscriptores, titulares y terceros que confían del cese con por lo menos treinta (30) días calendario de anticipación.
- Transferirá sus obligaciones relativas al mantenimiento de la información de registro y de los registros de auditoría durante el periodo de tiempo indicado en la CPS.
- Las claves privadas de la EC 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.

7 CONTROLES TÉCNICOS DE SEGURIDAD

7.1 GENERACIÓN E INSTALACIÓN DEL PAR DE CLAVES

7.1.1 GENERACIÓN DEL PAR DE CLAVES DE LA EC

La generación del par de claves de la EC raíz y la subordinada fueron realizadas por personal de confianza capacitados.

Para la EC raíz y la EC Subordinada de LLAMA.PE:

1. Se realizó con un dispositivo HSM ULTIMACO CRYPTOSERVER SE500 LAN V4C que cumple con la certificación FIPS 140 2 – LEVEL 3 de acuerdo al número de certificado 2814.
2. La generación de las claves de la EC se realizó en un entorno seguro por el personal adecuado según los roles de confianza y con un control dual.
3. Los pares de claves de la EC se generarán en una ceremonia de generación de claves de conformidad con los requisitos exigidos por INDECOPI.
4. El personal de confianza de la EC que participó de la generación de claves se identifica apropiadamente y registró todas las actividades que hayan sido realizadas con los fines de seguimiento que la Gerencia de LLAMA.PE considere adecuado.
5. El procedimiento completo de la generación de claves fue grabado, tanto a nivel de la sala donde se ejecutó, como la pantalla de la estación de trabajo durante toda la ejecución del procedimiento.
6. El custodio de los materiales criptográficos tiene un inventario de todos los dispositivos que fueron utilizados para la generación de claves, vigilando que ninguno de estos haya sido manipulado y/o reemplazado.
7. El equipo está ubicado y protegido para reducir los riesgos de amenazas, peligros ambientales y del acceso no autorizado.
8. La energía y telecomunicaciones está protegido de intercepción o daño.

7.1.2 GENERACIÓN DEL PAR DE CLAVES DE LA TSA

LLAMA.PE realiza los esfuerzos que razonablemente estén a su alcance para confirmar que las claves de la TSA sean generadas de acuerdo a los estándares.

En particular:

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

7.1.3 GENERACIÓN DEL PAR DE CLAVES DEL SUSCRIPTOR

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

Si las claves del Firmante/Suscriptor son generadas por la AC, ésta deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que las claves son generadas de forma segura y que se mantendrá la privacidad de estas.

En particular:

1. Las claves serán generadas usando un algoritmo SHA 256 RSA para los propósitos de la firma electrónica avanzada.
2. Las claves tendrán una longitud de 2048 bits.
3. Las claves serán generadas y guardadas de forma segura antes de entregárselas al Firmante/Suscriptor.
4. Las claves serán destruidas de forma segura después de su entrega al Firmante/Suscriptor.

7.1.4 ENTREGA DE LA CLAVE PÚBLICA AL SUSCRIPTOR

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

La clave privada será almacenada en un medio software (p. ej. PKCS12).

Cuando la EC entrega en un medio software donde esté asociado unos datos de activación del Tercero que confía (p. ej. Un código PIN), los datos de activación se deberán preparar de forma segura y distribuirse de manera separada del dispositivo seguro de creación de firma.

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

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

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

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

La EC mantiene la integridad y la autenticidad de la clave pública y los parámetros que se encuentren asociados a ella durante su distribución a los Terceros que confían.

En particular:

La EC, proporciona la cadena de certificados completa (raíz - subordinada- usuario final).

7.1.7 TAMAÑO Y PERIODO DE VALIDEZ DE LAS CLAVES DEL EMISOR

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

El periodo de uso de una clave privada será como máximo de 20 años, después del cual deberán cambiarse estas claves.

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

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

7.1.8 TAMAÑO Y PERIODO DE VALIDEZ DE LAS CLAVES DEL SUSCRIPTOR

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

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

7.1.9 HARDWARE/SOFTWARE DE GENERACIÓN DE CLAVES

Las claves de la EC serán generadas en un módulo criptográfico HSM ULTIMACO CRYPTOSERVER SE500 LAN V4C validado con la certificación FIPS 140 2 – LEVEL 3.

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

7.1.10 FINES DEL USO DE LA CLAVE

La EC deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que las claves de firma de la EC son usadas para:

- Firma Digital
- Firma de Certificados
- Firma de CRL

La clave privada del Suscriptor deberá ser usada para:

- Autenticación del suscriptor
- Firma y no repudio
- Correo seguro

7.2 PROTECCIÓN DE LA CLAVE PRIVADA

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

1. La clave privada de firma de la EC será mantenida y usada en un dispositivo criptográfico seguro, HSM ULTIMACO CRYPTOSERVER SE500 LAN V4C validado con la certificación FIPS 140 2 – LEVEL 3.
2. Cuando la clave privada de la EC esté fuera del módulo criptográfico esta estará cifrada
3. Se hará un backup de la clave privada de firma de la EC, que será almacenada y recuperada sólo por el personal autorizado según los roles de confianza, usando al menos un control dual en un medio físico seguro. El personal autorizado para desempeñar estas funciones estará limitado a aquellos requerimientos desarrollados en la CPS

De la TSA

LLAMA.PE realiza los esfuerzos que razonablemente estén a su alcance para confirmar que las claves privadas de la TSU continúan siendo confidenciales y mantienen su integridad.

En particular:

1. La clave privada de firma de la TSA será mantenida y usada en un dispositivo criptográfico seguro, el cual cumple los requerimientos que se detallan en el FIPS 140-2, en su nivel 3
2. Cuando la clave privada de la TSA esté fuera del módulo criptográfico esta deberá estar cifrada

3. Se deberá hacer un back up de la clave privada de firma de la TSA, que deberá ser almacenada y recuperada sólo por el personal autorizado según los roles de confianza, usando, al menos un control dual en un medio físico seguro. El personal autorizado para desempeñar estas funciones estará limitado a aquellos requerimientos desarrollados en la Política de Seguridad de LLAMA.PE.

Las copias de back up de la clave privada de firma de la TSA se regirán por el mismo o más alto nivel de controles de seguridad que las claves que se usen en ese momento.

Del Titular/Suscriptor

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

- el Titular/Suscriptor pueda mantener la clave privada bajo su exclusivo control.
- la clave privada puede ser efectivamente protegida por el Titular/Suscriptor contra un uso ajeno.

7.3 ESTÁNDARES PARA MÓDULOS CRIPTOGRÁFICOS

Todas las operaciones criptográficas son desarrolladas en un módulo validado con el nivel 3 de FIPS 140-2.

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

La EC, ha implementado procedimientos que requieren la participación de al menos 4 de 2 personas de confianza para llevar a cabo las operaciones criptográficas.

7.3.2 CUSTODIA DE LA CLAVE PRIVADA

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

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

7.3.3 BACKUP DE LA CLAVE PRIVADA

La EC crea copias de seguridad de su propia clave privada para poder hacer posible su recuperación en caso de cualquier eventualidad como pérdida, deterioro o desastre.

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

7.3.4 ARCHIVO DE LA CLAVE PRIVADA

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

7.3.5 INTRODUCCIÓN DE LA CLAVE PRIVADA EN EL MÓDULO CRIPTOGRÁFICO

La clave privada de la EC se creó dentro de un módulo criptográfico seguro, HSM ULTIMACO CRYPTOSERVER SE500 LAN V4C con certificación FIPS 140-2 – Level 3 de propiedad de LLAMA.PE.

La recuperación de la clave privada en el módulo criptográfico se realizará al menos con 2 de las 4 personas de confianza autorizados para realizar dicha acción.

7.3.6 MÉTODO DE ACTIVACIÓN DE LA CLAVE PRIVADA

Los datos de activación serán entregados al suscriptor por medio de un canal seguro.

Los suscriptores deberán proteger el acceso a su clave privada por medio de una contraseña, está deberá ser memorizada por el Suscriptor y no debe ser anotada en un lugar de fácil acceso ni compartidos.

7.3.7 MÉTODO DE DESACTIVACIÓN DE LA CLAVE PRIVADA

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

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

7.3.8 MÉTODO PARA DESTRUIR LA CLAVE PRIVADA

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

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

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

La destrucción de la clave privada la realizará el personal de confianza de la siguiente manera:

1. En la fecha de expiración se eliminará la clave privada y las copias de respaldo mediante el RESET del módulo criptográfico y la clave maestra, se guardará la clave pública y se hará una publicación en la página web de Llama.pe indicando que se trata de una versión anterior.
2. Se solicita un nuevo certificado y se repite los pasos de generación de claves.
3. Se comunica a todos los terceros que confían mediante mensajes de correo electrónico y se publicará en el repositorio que el certificado ha sido expirado

7.4 OTROS ASPECTOS DE LA GESTIÓN DEL PAR DE CLAVES

7.4.1 ARCHIVO DE LA CLAVE PÚBLICA

La EC deberá conservar todas las claves públicas de verificación.

7.5 DATOS DE ACTIVACIÓN

7.5.1 GENERACIÓN E INSTALACIÓN DE LOS DATOS DE ACTIVACIÓN

Los datos de activación de las EC se generan y se almacenan en tarjetas inteligentes criptográficas de ULTIMACO debidamente seriadas, utilizadas únicamente por el personal de confianza autorizado.

7.5.2 PROTECCIÓN DE LOS DATOS DE ACTIVACIÓN

Solo el personal de confianza autorizado conoce el procedimiento de la activación de datos que es mediante contraseñas y PINs para poder acceder.

7.5.3 OTROS ASPECTOS DE LOS DATOS DE ACTIVACIÓN

No estipulados.

7.6 CICLO DE VIDA DEL DISPOSITIVO SEGURO DE ALMACENAMIENTO DE LOS DATOS DE CREACIÓN DE FIRMA (DSADCF) Y DEL DISPOSITIVO SEGURO DE CREACIÓN DE FIRMA (DSCF)

La EC deberá, por sí misma o por delegación de esta función, realizar los mayores esfuerzos para asegurar que:

1. La preparación del DSADCF o DSCF es controlada de forma segura.

2. El DSADCF o DSCF es almacenado y distribuido de forma segura.
3. Si el propio sistema lo permite, que la activación y desactivación del DSADCF o DSCF es controlada de forma segura
4. El DSADCF o DSCF no es usado por la EC o entidad delegada antes de su emisión
5. El DSADCF o DSCF queda inhabilitado para su uso en caso de ser devuelto por el Suscriptor.
6. Cuando el DSADCF o DSCF lleve asociado unos datos de activación (ej PIN), estos datos de activación y el dispositivo seguro de creación de firma serán preparados y distribuidos de forma separada.

7.7 CONTROLES DE SEGURIDAD INFORMÁTICA

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

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

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

7.7.1 REQUISITOS TÉCNICOS DE SEGURIDAD ESPECÍFICOS

Cada servidor de LLAMA.PE incluye las siguientes funcionalidades:

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

7.7.2 EVALUACIÓN DE LA SEGURIDAD INFORMÁTICA

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

7.7.3 MANTENIMIENTO DE SERVIDORES DE LA AC

La Raíz Llama.pe ROOT CA se encuentra siempre Offline.

La subordinada Llama.pe SHA256 Standard CA y la TSA se apagará en caso se presente las siguientes circunstancias:

- -Se haga un mantenimiento preventivo del servidor.
- Haya un reinicio no programado del servidor.
- Se presente la pérdida de energía en el centro de datos, entre otros.

7.8 CONTROLES TÉCNICOS DEL CICLO DE VIDA

7.8.1 CONTROLES DE DESARROLLO DE SISTEMAS

En cuanto al control de cambios en el sistema, LLAMA.PE procede a realizar pruebas previo a su aceptación para luego ser publicada la versión final.

En principio, los cambios en el sistema se cargan en un repositorio, dicha versión se descarga para las respectivas pruebas, se comunica al Área de producción y esta misma versión se carga al servidor. Este repositorio permite evidenciar el historial de versiones, realizar roll out y roll back.

En caso de requerir un sistema tercerizado, LLAMA.PE se asegurará de que también se emplee un adecuado control de desarrollo de sistemas.

7.8.2 CONTROLES DE DESARROLLO DE SOFTWARE

LLAMA.PE procede a realizar pruebas al software previo a su aceptación para luego ser publicada la versión final. El procedimiento es el mismo que se describe para el desarrollo de sistemas.

De igual manera, en caso de requerir un software tercerizado, LLAMA.PE se asegurará de que también se emplee un adecuado control de desarrollo de software.

7.8.3 CONTROLES DE GESTIÓN DE SEGURIDAD

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

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

7.8.4 CONTROLES DE SEGURIDAD DEL CICLO DE VIDA

No estipulado.

7.9 CONTROLES DE SEGURIDAD DE LA RED

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

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

8 AUDITORÍA DE CONFORMIDAD Y OTROS CONTROLES

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

8.1 FRECUENCIA O CIRCUNSTANCIAS DE LOS CONTROLES

LLAMA.PE lleva a cabo auditorías internas y externas. Las auditorías internas se llevarán a cabo al menos dos veces al año y las evaluaciones técnicas del INDECOPI se llevarán a cabo una vez al año y cada vez que el INDECOPI lo requiera.

8.2 IDENTIDAD/CALIFICACIÓN DEL AUDITOR

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

8.3 RELACIÓN ENTRE EL AUDITOR Y LA ENTIDAD AUDITADA

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

8.4 ASPECTOS CUBIERTOS POR LOS CONTROLES

En líneas generales, las auditorías verifican:

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

8.5 TRATAMIENTOS DE LOS INFORMES DE AUDITORÍA

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

9 CONFORMIDAD

Esta Política de Seguridad ha sido aprobada por el Responsable de la EC, ER y TSA de LLAMA.PE. Cada vez que se genere un cambio en este documento, se procederá a informar previamente a INDECOPI y al dar conformidad, será nuevamente aprobada por el Responsable de la EC, ER y TSA.

10 BIBLIOGRAFÍA

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