POLÍTICA DE SEGURIDAD - SELLO DE TIEMPO

VERSIÓN: V1.0

PUBLICO

OFICIAL

TSA-POL-001

PARA: LLAMA.PE

HISTORIAL DE VERSIONES

VERSIÓN	DESCRIPCIÓN	REALIZADO POR	FECHA DE APROBACIÓN	FECHA DE REVISIÓN
V1.0	Version inicial	LOUIE DIAZ MARTICORENA	2026-10-29	2026-10-29

Documentos de Herencia

No tiene documentos de herencia.

Documentos de Referencia

- TSA-POL-002 POLITICA DE SELLADO DE TIEMPO

Tabla de contenido

- 1. OBJETIVO
- 2. ALCANCE
- 3. PRINCIPIOS DE SEGURIDAD
- 4. GOBIERNO, RESPONSABILIDADES Y APROBACIÓN
  - 4.1. APROBACIÓN DE LA POLÍTICA
  - 4.2. RESPONSABLE DE LA TSA
  - 4.3. RESPONSABLE DE SEGURIDAD / SGSI
  - 4.4. RESPONSABLE DE TI Y ADMINISTRADORES
  - 4.5. PERSONAL CON ROLES DE CONFIANZA
  - 4.6. PERSONAL, PROVEEDORES Y TERCEROS
- 5. EVALUACIÓN Y TRATAMIENTO DE RIESGOS
- 6. CONTROL DE ACCESO
- 7. SEGURIDAD DEL PERSONAL
- 8. SEGURIDAD FÍSICA Y AMBIENTAL
- 9. SEGURIDAD DE COMUNICACIONES Y REDES
- 10. MANTENIMIENTO DE EQUIPOS Y DESECHO
- 11. CONTROL DE CAMBIOS Y CONFIGURACIÓN
- 12. PLANIFICACIÓN DE CONTINGENCIAS Y CONTINUIDAD
- 13. AUDITORÍAS, REGISTROS Y DETECCIÓN DE INTRUSIONES
- 14. MEDIOS DE ALMACENAMIENTO, RESPALDO Y RECUPERACIÓN
- 15. PRIVACIDAD Y PROTECCIÓN DE LA INFORMACIÓN
- 16. GESTIÓN DE INCIDENTES Y COMUNICACIONES
- 17. CUMPLIMIENTO, EXCEPCIONES Y MEDIDAS CORRECTIVAS
- 18. DIFUSIÓN, REVISIÓN Y CONTROL DOCUMENTAL

1. OBJETIVO

Establecer los principios, responsabilidades y requisitos generales de seguridad aplicables a la Autoridad de Sellado de Tiempo (TSA) de LLAMA.PE S.A., con el propósito de proteger la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información, los sistemas, las claves criptográficas, los registros y los procesos que soportan la emisión y gestión de sellos de tiempo.

Esta política constituye el marco de seguridad de la TSA y se complementa con los procedimientos, planes, registros y controles operativos aprobados por LLAMA.PE.

2. ALCANCE

La política se aplica a la infraestructura, instalaciones, personal, sistemas, redes, componentes criptográficos, servicios tecnológicos, registros y procesos utilizados para prestar el servicio de sellado de tiempo de LLAMA.PE. Incluye la Unidad de Sellado de Tiempo (TSU), los sistemas que reciben y procesan solicitudes, los mecanismos de sincronización horaria, la gestión de certificados y claves, el almacenamiento y conservación de registros, los respaldos, la administración de cambios y la gestión de incidentes.

Es de cumplimiento obligatorio para trabajadores, administradores, operadores, titulares de roles de confianza, proveedores y terceros que, por autorización contractual o funcional, accedan a activos o información comprendidos en el alcance.

La política se dirige también a establecer compromisos de seguridad que respalden la confianza de solicitantes, suscriptores, usuarios y terceros que confían en los sellos de tiempo emitidos por LLAMA.PE.

3. PRINCIPIOS DE SEGURIDAD

- Confidencialidad: la información y los materiales criptográficos solo serán accesibles por personas, procesos o sistemas autorizados.
- Integridad: los sellos de tiempo, los registros, la configuración y la información asociada deben protegerse frente a alteraciones no autorizadas.
- Disponibilidad: los sistemas y datos necesarios para la prestación del servicio deben mantenerse disponibles conforme a los niveles de servicio y a los planes aprobados.
- Autenticidad y trazabilidad: las operaciones relevantes deben poder atribuirse a identidades autorizadas y reconstruirse mediante registros protegidos.
- Mínimo privilegio y necesidad de conocer: los permisos se limitarán a los requeridos para cumplir funciones autorizadas.

- Control dual y segregación de funciones: las operaciones críticas sobre claves y componentes criptográficos se ejecutarán con los controles compartidos que correspondan.
- Gestión basada en riesgos: los controles se seleccionarán, priorizarán y revisarán según la evaluación de riesgos vigente.
- Cumplimiento: las operaciones de la TSA deben observar los requisitos legales, regulatorios, contractuales y técnicos aplicables.

4. GOBIERNO, RESPONSABILIDADES Y APROBACIÓN

4.1. APROBACIÓN DE LA POLÍTICA

La Gerencia General, o la autoridad formalmente designada por LLAMA.PE, es responsable de aprobar esta política, sus modificaciones sustanciales y las excepciones que correspondan. La autoridad aprobadora debe confirmarse en la versión controlada antes de su entrada en vigor.

4.2. RESPONSABLE DE LA TSA

El Responsable de la TSA es responsable de promover la implementación de esta política en los procesos del servicio de sellado de tiempo, coordinar su revisión, asegurar su difusión y verificar que existan documentos operativos y evidencias de cumplimiento. La documentación TSA-POL-002 y TSA-DEC-001 identifica responsabilidades de LLAMA.PE sobre la implementación, revisión, actualización, difusión y capacitación relacionadas con sus prácticas.

4.3. RESPONSABLE DE SEGURIDAD / SGSI

El Responsable de Seguridad o responsable del SGSI, según la designación vigente, coordina la evaluación y tratamiento de riesgos, supervisa la aplicación de controles, revisa incidentes, promueve auditorías y reporta desviaciones a la dirección. La asignación exacta de funciones y suplencias debe quedar documentada.

4.4. RESPONSABLE DE TI Y ADMINISTRADORES

El personal de TI administra los sistemas, redes, equipos, configuraciones, registros, respaldos y mecanismos de monitoreo conforme a autorizaciones documentadas. No podrá ejecutar operaciones criptográficas reservadas a roles de confianza si no cuenta con la designación y autorización correspondientes.

4.5. PERSONAL CON ROLES DE CONFIANZA

Las personas asignadas a roles de confianza deben cumplir los requisitos de idoneidad, confidencialidad, capacitación y autorización aplicables. Las operaciones de generación, activación, instalación y gestión de claves de la TSU se limitarán al personal autorizado y se ejecutarán bajo control dual y en un ambiente físico seguro.

4.6. PERSONAL, PROVEEDORES Y TERCEROS

Todo personal y tercero con acceso a activos de la TSA debe cumplir esta política, los acuerdos de confidencialidad, las condiciones de acceso y las obligaciones contractuales de seguridad. Los accesos de terceros deben autorizarse, limitarse al alcance contratado y revisarse durante la relación de servicio.

5. EVALUACIÓN Y TRATAMIENTO DE RIESGOS

La TSA mantendrá una evaluación de riesgos documentada cuyo alcance comprenda los procesos y activos relevantes para el sellado de tiempo. La evaluación debe identificar y valorar activos, amenazas, vulnerabilidades, impactos, probabilidad y nivel de riesgo, y establecer el tratamiento de los riesgos moderados y graves, como mínimo, de acuerdo con el criterio aprobado por LLAMA.PE.

Los controles de esta política deben sustentarse en dicha evaluación. Los riesgos residuales, sus responsables, las medidas de tratamiento, los plazos y las aceptaciones deberán quedar registrados y aprobados por los roles organizacionales competentes.

La evaluación se revisará ante cambios significativos en la infraestructura, proveedores, procesos, tecnología criptográfica, requisitos legales, incidentes relevantes o cambios en el contexto del servicio.

Responsable de aprobación: Gerencia General o autoridad delegada, según el procedimiento de gestión de riesgos. Responsable de implementación: Responsable de Seguridad/SGSI, con los propietarios de activos y procesos. Documentos de soporte: metodología y matriz de riesgos, plan de tratamiento, declaración de aplicabilidad cuando corresponda y registros de aceptación de riesgos.

6. CONTROL DE ACCESO

El acceso lógico y físico a información, aplicaciones, sistemas, equipos, redes, instalaciones y materiales criptográficos de la TSA debe concederse exclusivamente a identidades autorizadas, con base en funciones, necesidad de conocer, mínimo privilegio y resultados de la evaluación de riesgos.

- Cada usuario debe utilizar una identidad individual, salvo cuentas técnicas justificadas, documentadas y sujetas a controles reforzados.

- Las altas, modificaciones, revisiones y bajas de accesos deben ser autorizadas y registradas; los permisos deben retirarse oportunamente cuando dejan de ser necesarios.

- Los accesos privilegiados deben limitarse, protegerse y revisarse periódicamente; las actividades administrativas relevantes deben registrarse.

- El acceso a claves privadas de la TSU y a funciones criptográficas críticas debe restringirse a roles de confianza formalmente designados y aplicar control dual.

- El acceso a ambientes que alojan información sensible o componentes críticos debe estar restringido y contar con registros de ingreso cuando corresponda.

- La información física y electrónica debe protegerse contra lectura, modificación, copia, traslado o eliminación no autorizados.

Responsable de aprobación: Gerencia General o autoridad delegada. Responsable de implementación: Responsable de TI y responsables de los activos, con supervisión del Responsable de Seguridad. Documentos de soporte: política y matriz de control de acceso, procedimiento de gestión de identidades y accesos, matriz de roles, registros de autorización y revisión de permisos.

7. SEGURIDAD DEL PERSONAL

- LLAMA.PE debe establecer controles de seguridad de personal proporcionales a las funciones y al riesgo, especialmente para los roles de confianza y el personal con acceso privilegiado o criptográfico.

- Verificar la identidad, experiencia, referencias y antecedentes que resulte legalmente procedente y proporcional al puesto, antes de asignar funciones de confianza.

- Definir perfiles de puesto, responsabilidades, autorizaciones, incompatibilidades y obligaciones de confidencialidad.

- Formalizar la aceptación de las políticas y obligaciones de seguridad por parte del personal y terceros.

- Proporcionar capacitación inicial y periódica en seguridad de la información, privacidad, uso aceptable, control de acceso, incidentes y responsabilidades específicas de la TSA.

- Establecer un mecanismo para comunicar incidentes, debilidades, sospechas de compromiso o incumplimientos sin demora.

- Retirar o modificar accesos, credenciales, autorizaciones y activos asignados cuando finalice o cambie la relación laboral o contractual.

Responsable de aprobación: Gerencia General. Responsable de implementación: responsable de gestión de personas y responsables de área, con apoyo del Responsable de Seguridad. Documentos de soporte: procedimiento de selección y seguridad de personal, perfiles de puestos, acuerdos de confidencialidad, registros de capacitación y listas de roles de confianza.

8. SEGURIDAD FÍSICA Y AMBIENTAL

Las instalaciones y ambientes que alojan sistemas, información o componentes de la TSA deben protegerse frente a acceso no autorizado, robo, manipulación, incendio, fallas ambientales, interrupciones de energía y otros eventos que puedan afectar la seguridad o continuidad del servicio.

- Definir zonas y niveles de acceso según la criticidad de los activos y mantener autorizaciones de ingreso actualizadas.
- Aplicar controles de ingreso físico y conservar registros de acceso a áreas restringidas, según el riesgo.
- Proteger los equipos críticos frente a manipulación, daño, pérdida y condiciones ambientales fuera de los rangos operativos.
- Mantener controles de energía, climatización, detección y respuesta ante eventos físicos de acuerdo con el diseño de las instalaciones.
- Controlar llaves, tarjetas, credenciales físicas y otros medios de acceso; reportar de inmediato su pérdida o compromiso.
- Retirar y eliminar de forma segura documentos, soportes y equipos en desuso que hayan contenido información sensible.
- Asegurar que el transporte, instalación, mantenimiento y retiro de módulos criptográficos se realice bajo controles documentados.

Responsable de aprobación: Gerencia General o autoridad delegada. Responsable de implementación: responsable de infraestructura/administración y Responsable de TI. Documentos de soporte: procedimiento de seguridad física y ambiental, registro de visitas, matriz de áreas restringidas, mantenimiento de instalaciones y plan de contingencia.

9. SEGURIDAD DE COMUNICACIONES Y REDES

- Las comunicaciones internas y externas que soportan la TSA deben protegerse para prevenir accesos no autorizados, alteración, divulgación, suplantación, interrupción y uso indebido. La arquitectura de red y las medidas de protección deben corresponder a la evaluación de riesgos.
- Separar, cuando corresponda, los entornos de administración, operación, monitoreo y servicios expuestos, restringiendo los flujos de comunicación a los necesarios.
- Proteger las conexiones administrativas y de terceros mediante mecanismos de autenticación y cifrado adecuados al riesgo.
- Gestionar reglas de cortafuegos, accesos remotos, servicios expuestos y cambios de red mediante autorización y registro.

- Mantener mecanismos de protección, registro y monitoreo para detectar actividad anómala, intentos de intrusión y eventos que afecten la disponibilidad.

- Establecer requisitos de seguridad para proveedores y otros medios de comunicación que interactúen con la TSA.

- Proteger la sincronización horaria y la comunicación con las fuentes de tiempo autorizadas; monitorear desviaciones y fallos.

- Ante sospecha de compromiso de operaciones, de la clave privada de firma o pérdida de calibración temporal, suspender la emisión cuando corresponda y comunicar el evento a las partes interesadas según las prácticas vigentes.

- Responsable de aprobación: Gerencia General o autoridad delegada. Responsable de implementación: Responsable de TI, con supervisión del Responsable de Seguridad y del Responsable de la TSA. Documentos de soporte: política de seguridad de redes, diagramas de red, reglas de filtrado, procedimiento de acceso remoto, gestión de vulnerabilidades, monitoreo y gestión de incidentes.

10. MANTENIMIENTO DE EQUIPOS Y DESECHO

- Los equipos y componentes de hardware y software que soportan la TSA deben mantenerse en condiciones seguras durante su adquisición, instalación, operación, mantenimiento, traslado, sustitución y retiro. Las intervenciones deben ser realizadas por personal autorizado y dejar evidencia proporcional a su criticidad.

- Mantener un inventario de equipos, sistemas, componentes criptográficos, responsables, ubicación y estado del ciclo de vida.

- Planificar y registrar mantenimientos preventivos y correctivos, así como las intervenciones de proveedores.

- Verificar la autorización, identidad y alcance de los técnicos antes de permitir intervenciones en activos críticos.

- Proteger la información durante reparación, transporte o diagnóstico; evitar que proveedores accedan a información o claves no necesarias.

- Antes de reutilizar, devolver o desechar un equipo o soporte, eliminar de forma segura la información y las credenciales que contenga.

- En el caso de equipos criptográficos, gestionar las claves de acuerdo con su estado y vigencia; cuando corresponda el retiro, impedir su uso no autorizado y asegurar la destrucción de claves vencidas o revocadas conforme a los procedimientos aplicables.

- Conservar constancias de mantenimiento, devolución, borrado seguro, destrucción o disposición final.

- Responsable de aprobación: Gerencia General o autoridad delegada. Responsable de implementación: Responsable de TI y responsable de infraestructura. Documentos de soporte: inventario de activos, procedimiento de mantenimiento, gestión de proveedores, procedimiento de borrado seguro y disposición de activos, registros de intervención.

11. CONTROL DE CAMBIOS Y CONFIGURACIÓN

- Los cambios que puedan afectar la seguridad, integridad, precisión temporal, disponibilidad o conformidad del servicio de la TSA deben evaluarse, aprobarse, probarse, documentarse y verificarse antes de su puesta en producción, salvo el tratamiento de emergencia definido y aprobado por el procedimiento correspondiente.

- Identificar el motivo, alcance, activos afectados, riesgos, impacto en el servicio y plan de reversión de cada cambio.

- Obtener aprobación previa de una persona con autoridad definida y mantener separación entre solicitud, aprobación e implementación cuando sea viable.

- Probar los cambios en un entorno adecuado antes de su despliegue, y documentar resultados y aceptación.

- Mantener configuraciones base seguras, control de versiones y registros de cambios en sistemas críticos.

- Gestionar cambios de software, firmware, parámetros criptográficos, reglas de red, certificados, fuentes de tiempo y componentes de la TSU con controles acordes a su criticidad.

- Revisar los cambios de emergencia después de su implementación y conservar la justificación y evidencia.

- Responsable de aprobación: propietario del sistema o autoridad de cambios designada. Responsable de implementación: Responsable de TI y personal técnico autorizado. Documentos de soporte: procedimiento de gestión de cambios, registro de cambios, inventario de configuración, resultados de pruebas y planes de reversión.

12. PLANIFICACIÓN DE CONTINGENCIAS Y CONTINUIDAD

- La TSA debe disponer de medidas de contingencia proporcionales a los riesgos identificados para responder a interrupciones, fallos de infraestructura, indisponibilidad de proveedores, desviaciones de tiempo, incidentes de seguridad o sospecha de compromiso de claves y operaciones.

- Definir escenarios de interrupción y criterios para detener la emisión de sellos de tiempo cuando no pueda garantizarse la seguridad o precisión requerida.

- Establecer responsabilidades, escalamiento, canales de comunicación y criterios para declarar una contingencia.

- Mantener procedimientos de recuperación de sistemas, configuración, información y registros, con objetivos de recuperación aprobados.

- Probar periódicamente los planes y documentar resultados, deficiencias y acciones correctivas.

- Cuando exista sospecha de compromiso de la clave privada de firma o pérdida de calibración del servicio, interrumpir la emisión y comunicar a las partes interesadas mediante los canales definidos.

- En caso de cese planificado de la TSA, gestionar con anticipación las comunicaciones, la conservación de registros, la disponibilidad de certificados y la destrucción segura de las claves privadas, de acuerdo con las prácticas aprobadas.

- Responsable de aprobación: Gerencia General. Responsable de implementación: Responsable de la TSA, Responsable de TI y Responsable de Seguridad, de acuerdo con sus funciones. Documentos de soporte: análisis de impacto, plan de continuidad y recuperación, plan de respuesta a incidentes, pruebas de recuperación y procedimiento de interrupción/cese del servicio.

13. AUDITORÍAS, REGISTROS Y DETECCIÓN DE INTRUSIONES

- La TSA debe someter sus controles, sistemas, procesos y registros a revisiones y auditorías periódicas, así como mantener mecanismos para detectar, registrar, analizar y escalar eventos de seguridad relevantes.

- Definir el objetivo, alcance, frecuencia, criterios y responsables de auditorías internas y externas aplicables.

- Proteger los registros de eventos frente a acceso, modificación, eliminación o pérdida no autorizados.

- Registrar eventos relevantes de seguridad, administración, acceso privilegiado, cambios, operaciones criptográficas y disponibilidad, según el alcance y riesgo.

- Monitorear alertas e indicadores de intrusión, fallos de servicio, anomalías de tiempo y eventos que puedan comprometer la TSU.

- Investigar desviaciones e incidentes, documentar conclusiones y realizar seguimiento de acciones correctivas.

- Conservar los registros de eventos y auditoría durante los periodos establecidos en la documentación normativa y las obligaciones legales o contractuales aplicables.

- Restringir el acceso a los resultados de auditoría y comunicar los hallazgos a los responsables autorizados.

- Responsable de aprobación: Gerencia General. Responsable de implementación: Responsable de Seguridad/SGSI y Responsable de la TSA, con apoyo de TI. Documentos de soporte: programa de auditoría, procedimiento de registro y monitoreo, catálogo de eventos, registros de incidentes, informes de auditoría y seguimiento de acciones correctivas.

14. MEDIOS DE ALMACENAMIENTO, RESPALDO Y RECUPERACIÓN

- Los medios de almacenamiento que contengan información de la TSA deben administrarse para proteger su confidencialidad, integridad, disponibilidad y trazabilidad durante su uso, transporte, respaldo, recuperación, archivo y eliminación.
- Clasificar la información y los soportes según su sensibilidad, criticidad y requisitos de conservación.
- Definir respaldos de la información, configuraciones, registros y componentes necesarios para recuperar el servicio, de acuerdo con la evaluación de riesgos.
- Proteger las copias de respaldo frente a acceso no autorizado, modificación, pérdida y destrucción, y mantener separación adecuada respecto del entorno principal.
- Restringir y registrar el acceso a medios y repositorios de respaldo; cifrar los respaldos cuando lo determine el riesgo o el requisito aplicable.
- Realizar pruebas periódicas de restauración y conservar evidencia de sus resultados.
- Controlar el traslado, devolución, reutilización y eliminación de medios; aplicar borrado seguro o destrucción cuando corresponda.
- Gestionar por separado las copias de seguridad de claves criptográficas conforme a los procedimientos específicos de ciclo de vida de claves, sin debilitar los controles de doble intervención ni la protección criptográfica.
- Responsable de aprobación: Gerencia General o autoridad delegada. Responsable de implementación: Responsable de TI y propietarios de la información, con supervisión del Responsable de Seguridad. Documentos de soporte: política y procedimiento de respaldo y recuperación, matriz de respaldos, registros de ejecución, pruebas de restauración, inventario de medios y procedimiento de eliminación segura.

15. PRIVACIDAD Y PROTECCIÓN DE LA INFORMACIÓN

La información personal que sea recolectada, almacenada, procesada, transferida o revelada en el marco de los servicios de LLAMA.PE debe tratarse para fines autorizados, limitarse a lo necesario, protegerse contra acceso no autorizado y gestionarse conforme a las obligaciones legales y compromisos de privacidad aplicables.

Los accesos a información personal deben restringirse según funciones y necesidad de conocer. Las solicitudes de acceso o corrección, las transferencias y las comunicaciones relacionadas con datos personales deben tramitarse por los procedimientos establecidos. Los incidentes que afecten información personal deben escalarse y gestionarse conforme al procedimiento de incidentes y a las obligaciones legales vigentes.

Responsable de aprobación: Gerencia General. Responsable de implementación: responsable de privacidad o función designada, junto con los responsables de procesos y el Responsable de Seguridad. Documentos de soporte: TSA-PLN-001 Plan de Privacidad TSA, avisos de privacidad, procedimiento de derechos de titulares, gestión de incidentes y acuerdos con encargados/proveedores.

16. GESTIÓN DE INCIDENTES Y COMUNICACIONES

- Todo evento o debilidad que pueda afectar la seguridad, la operación, la precisión temporal, las claves criptográficas, los registros o la información de la TSA debe reportarse, registrarse, evaluarse y tratarse sin demora injustificada.
- Establecer canales de reporte, responsables de recepción, clasificación, escalamiento y toma de decisiones.
- Preservar evidencias y registros pertinentes para la investigación, manteniendo su integridad y control de acceso.
- Aplicar medidas de contención y recuperación proporcionales al incidente, incluida la suspensión de la emisión cuando no se pueda garantizar la seguridad o precisión del sello.
- Determinar las partes que deben ser informadas, el contenido de la comunicación y el plazo aplicable conforme a las obligaciones regulatorias, contractuales y legales.
- Registrar la causa, el impacto, las decisiones adoptadas y las acciones correctivas; revisar la eficacia de las medidas.
- Comunicar las interrupciones relevantes a través de los canales oficiales establecidos para el servicio y mantener actualizada la información pública necesaria.
- Responsable de aprobación: Gerencia General o autoridad de crisis designada. Responsable de implementación: Responsable de Seguridad y Responsable de la TSA, con apoyo de TI, privacidad, legal y comunicaciones. Documentos de soporte: procedimiento de gestión de incidentes, matriz de escalamiento, plan de comunicaciones y registros de incidentes.

17. CUMPLIMIENTO, EXCEPCIONES Y MEDIDAS CORRECTIVAS

El cumplimiento de esta política es obligatorio para las personas y terceros incluidos en su alcance. Cualquier excepción debe justificarse por escrito, evaluar sus riesgos, establecer controles compensatorios, tener un plazo de vigencia y ser aprobada por la autoridad competente antes de su aplicación, salvo que un procedimiento de emergencia establezca otra cosa.

Los incumplimientos deben registrarse, evaluarse y tratarse mediante las medidas correctivas, contractuales, administrativas o disciplinarias que correspondan, respetando la legislación aplicable y los procedimientos internos.

Responsable de aprobación: Gerencia General. Responsable de implementación: responsables de área y Responsable de Seguridad. Documentos de soporte: procedimiento de no conformidades y acciones correctivas, registro de excepciones, matriz de cumplimiento y

acuerdos contractuales.

18. DIFUSIÓN, REVISIÓN Y CONTROL DOCUMENTAL

La política debe mantenerse bajo control documental, comunicarse a las personas comprendidas en su alcance y estar disponible para los responsables que deban aplicarla. La versión aprobada y sus cambios deben gestionarse de acuerdo con el proceso documental de LLAMA.PE y con los requisitos de comunicación o publicación aplicables a la TSA.

La política se revisará al menos una vez al año y cuando existan cambios relevantes en los servicios, tecnología, riesgos, proveedores, requisitos legales o regulatorios, incidentes significativos o resultados de auditoría. Las revisiones deben quedar registradas.

Responsable de aprobación: Gerencia General o autoridad formalmente delegada. Responsable de implementación: Responsable de la TSA y responsable de control documental. Documentos de soporte: procedimiento de control documental, historial de versiones, registro de difusión y constancias de capacitación.