llama.pe

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

VERSIÓN: V2.1

PUBLICO

OFICIAL

PARA: LLAMA.PE

HISTORIAL DE VERSIONES

VERSIÓN	DESCRIPCIÓN	REALIZADO POR	FECHA
V2.1	- se cambien los código de identificación de los documentos relacionados "AX-LLA-00X por "LLA-XXX-0XX" - se cambia la palabra política por cláusula en los párrafos correspondientes	LOUIE ALBERTO DIAZ MARTICORENA	2023-06-14
V2.0	- Se agrego los puntos 5.1 y 5.2 - Actualización del punto 5 (formato) - se actualiza los niveles de clasificación de la información 5.1.3 - se agrega el punto 6 mejora continua	LOUIE ALBERTO DIAZ MARTICORENA	2022-11-18
V1.0	Actualización del punto 5 (formato)	LOUIE ALBERTO DIAZ MARTICORENA	2020-10-30

Documentos de Referencia

No tiene documentos de referencia.

Tabla de contenido

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

1 OBJETIVO

El propósito de las Políticas de Seguridad es establecer principios, reglas y lineamientos básicos para la gestión de la seguridad de información en los servicios brindados por Llama.pe que son:

- Generación y validación de certificados digitales
- Servicio de firma digital
- Servicio de sello de tiempo.

2 ALCANCE Y USUARIOS

Esta Política se aplica a todo el Sistema de gestión de seguridad de la información, según se define en el documento del Alcance del SGSI.

Los usuarios de este documento son todos los empleados de Llama.pe, como también terceros externos a la organización.

3 DOCUMENTOS DE REFERENCIA

- Norma ISO/IEC 27001.
- Norma ISO/IEC 27002.
- Guia de acreditación INDECOPI
- Declaración de Aplicabilidad.
- Documento sobre el alcance del SGSI.

4 DEFINICIONES SOBRE SEGURIDAD DE LA INFORMACIÓN

Activo: Cualquier cosa, información o sistema relacionado con el tratamiento de la misma que tenga valor para la empresa.

Datos: Son todos aquellos elementos básicos de la información (en cualquier formato) que se generan, recogen, gestionan, transmiten y destruyen en Llama.pe.

Personal: Es todo el personal de Llama.pe, el personal subcontratado, usuarios y en general, todos aquellos que tengan acceso de una manera u otra a los activos de información de Llama.pe.

Servicios: Son los servicios internos, aquellos que una parte de la organización suministra a otra, como los externos, aquellos que la organización suministra a clientes y usuarios.

Acuerdo de Confidencialidad: documento que los gerentes y empleados de Llama.pe o los provistos por terceras partes manifiestan su voluntad de mantener la confidencialidad de la información de la empresa, comprometiéndose a no divulgar, usar o explotar la información confidencial a la que tengan acceso.

Alcance: Ámbito de la organización que queda sometido al SGSI. Debe incluir la identificación clara de las dependencias, interfaces y límites con el entorno, sobre todo si sólo incluye una parte de la organización.

Amenaza: Según [ISO/IEC 13335-1:2005]: causa potencial de un incidente no deseado, el cual puede causar daño a un sistema o la organización.

Auditoría: Proceso planificado y sistemático en el cual un auditor obtiene evidencias objetivas que le permitan emitir un juicio informado sobre el estado y efectividad del SGSI de una organización.

Autenticación: Proceso que tiene por objetivo asegurar la identificación de una persona o sistema.

Confidencialidad: acceso a la información por parte únicamente de quienes estén autorizados.

Control: toda actividad o proceso encaminado a mitigar o evitar un riesgo. Incluye políticas, procedimientos, guías, estructuras organizacionales y buenas prácticas, que pueden ser de carácter administrativo, tecnológico, físico o legal.

Criptografía: disciplina que agrupa a los principios, medios y métodos para la transformación de datos con el fin de ocultar el contenido de su información, establecer su autenticidad, prevenir su modificación no detectada, prevenir su repudio, y/o prevenir su uso no autorizado.

Desastre: Cualquier evento accidental, natural o malintencionado que interrumpe las operaciones o servicios habituales de una organización durante el tiempo suficiente como para verse afectada de manera significativa.

Política de seguridad: Documento que establece el compromiso de la Dirección y el enfoque de la organización en la gestión de la seguridad de la información. Según [ISO/IEC 27002]: intención y dirección general expresada formalmente por la Dirección.

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Según [ISO Guía 73:2009]: combinación de la probabilidad de un evento y sus consecuencias.

Riesgo Residual: Según [ISO/IEC Guía 73:2009] El riesgo que permanece tras el tratamiento del riesgo.

SGSI Sistema de Gestión de la Seguridad de la Información: Según [ISO/IEC 27001: 20013]: la parte de un sistema global de gestión que, basado en el análisis de riesgos, establece, implementa, opera, monitoriza, revisa, mantiene y mejora la seguridad de la información. (Nota: el sistema de gestión incluye una estructura de organización, políticas, planificación de actividades, responsabilidades, procedimientos, procesos y recursos.)

Usuario Externo: Persona que hace uso de las aplicaciones de Llama.pe en la web que no son trabajadores de Llama.pe.

Usuarios internos: Trabajadores o colaboradores de Llama.pe que tienen responsabilidad en una determinada área de la empresa, la que puede ser Sistemas, Soporte, Ventas, Finanzas, etc.

Vulnerabilidad: Debilidad en la seguridad de la información de una organización que potencialmente permite que una amenaza afecte a un activo. Según [ISO/IEC 13335-1:2004]: debilidad de un activo o conjunto de activos que puede ser explotado por una amenaza.

5 POLÍTICAS DE SEGURIDAD

5.1. LINEAMIENTOS DE GESTIÓN PARA LA SEGURIDAD DE LA INFORMACIÓN

El objetivo del presente apartado es brindar una guía y apoyo a la gestión de la seguridad de la información de acuerdo con las exigencias de la empresa, las normas y leyes relevantes.

5.1.1 POLÍTICAS PARA LA SEGURIDAD DE LA INFORMACIÓN

- La Gerencia diseña, programa y realiza los programas de auditoría del sistema de gestión de seguridad de la información, los cuales estarán a cargo del Oficial de Seguridad de la Información.
- Todo aplicativo informático o software es comprado, diseñado o aprobado por la Jefatura de Sistemas.
- Los jefes de área aseguran que todos los procedimientos de seguridad de la información dentro de su área de responsabilidad, se realizan correctamente para lograr el cumplimiento de las políticas y estándares de seguridad de la información de Llama.pe.
- El servicio de transferencia de archivos se realiza empleando protocolos seguros cuando el origen sea Llama.pe hacia entidades externas.

5.1.2 CONTROLES DE ACCESO

La gerencia, mediante el administrador del sistema, debe establecer los controles necesarios para acceder a las plataformas, aplicaciones e información que ellos contengan.

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 del Sistema deberá 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 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.

Se ha definido y establecido reglas de qué usuarios tendrán acceso a las redes y servicios. Estas reglas están en función a la definición de los perfiles de usuarios y funciones de cada puesto (Manual de Organización y Funciones de Llama.pe) estos controles son empleados para mitigar los riesgos de **Divulgación o alteración de información por acceso no autorizado a aplicativos y bases de datos**

Los demás puntos se inician en el documento **LLA-CLA-009**

5.1.3 CLASIFICACIÓN DE LA INFORMACIÓN

- El oficial de seguridad debe identificar los riesgos a los que está expuesta la información de las áreas, teniendo en cuenta que la información pueda ser copiada, divulgada, modificada o destruida física o digitalmente por personal interno o externo.
- El oficial de seguridad y el Administrador del sistema deben considerar las siguientes características independientemente del tipo de activo:

1) No es fácilmente reemplazable sin incurrir en costos, habilidades especiales, tiempo, recursos o la combinación de los anteriores.

2) Forma parte de la identidad de la empresa y sin el cual Llama.pe puede estar en algún nivel de riesgo.

3) Los niveles de clasificación de la información que se ha establecido son: PÚBLICO, CONFIDENCIAL y ALTAMENTE CONFIDENCIAL

Llama.pe categoriza la información de la siguiente forma:

- Público: Activos de información cuyo contenido no es sensible de acceso público y que su divulgación no genera impacto en la empresa.
- Confidencial: Activos de información cuyo contenido sólo debe ser de uso y divulgación para el personal interno de la empresa y que sólo podrán ser divulgados a terceras partes teniendo firmado un acuerdo de confidencialidad, siempre y cuando su divulgación no impacte a la empresa.
- Altamente confidencial: Activos de información cuyo contenido no debe ser divulgado ni distribuido a personas que no sean autorizadas y cuya difusión genere un impacto importante en la empresa, entre ellas: pérdida económica, sanción legal o pérdida de imagen.

Los demás puntos se inician en el documento **LLA-CLA-008**

5.1.4 SEGURIDAD FÍSICA Y DEL ENTORNO

LLAMA.PE tiene como objetivo de seguridad, garantizar la Confidencialidad, integridad y disponibilidad de la información crítica de los procesos de registro, mediante la gestión de riesgos de seguridad y la aplicación de políticas y estándares que regulen las actividades críticas de las operaciones de sellado de tiempo, por parte del personal y terceros subcontratados, en cumplimiento de las obligaciones de Llama.pe en los ámbitos legales, regulatorios y contractuales.

Los controles son definidos en base a la identificación y valoración de los activos que forman parte de las operaciones de registro, así como la identificación de amenazas y vulnerabilidades de estos activos críticos, la evaluación del impacto de los riesgos, y el tratamiento de los riesgos de impacto grave y moderado que puedan presentarse en los procesos de registro contemplados por la ER de LLAMA.PE.

Los demás puntos se inician en el documento **LLA-CLA-011**

5.1.4.1 UBICACIÓN Y CONSTRUCCIÓN DEL LOCAL

La ubicación y diseño de las instalaciones de la ER de LLAMA.PE debe prever el daño por desastres naturales, como inundación, terremoto; así como desastres creados por el hombre, como incendios, disturbios civiles y otras formas de desastre, manteniendo vigente

su acreditación ante el Instituto Nacional de Defensa Civil.

Los demás puntos se inician en el documento **LLA-CLA-011**

5.1.5 SEGURIDAD DE LOS RECURSOS HUMANOS

- Se debe asegurar que los Jefes de Oficinas, terceros y demás colaboradores de Llama.pe, entiendan sus responsabilidades en relación con el SGSI de Llama.pe, esto se realizará mediante:
  - Capacitaciones (plan de capacitación)
  - Concientización (plan de concientización)
  - Estableciendo en sus contratos las cláusulas de confidencialidad y sanciones.
- y actúen de manera consistente frente a las mismas, con el fin de mitigar el riesgo de hurto, fraude, filtraciones o uso inadecuado de la información o los equipos empleados para el tratamiento de la información.

Los demás puntos se inician en el documento **LLA-CLA-007**

5.1.6 POLÍTICAS ESPECIFICAS PARA LOS USUARIOS DE LLAMA.PE

- Llama.pe debe almacenar su información en físico (cajas ignífugas) y/o en la nube con los permisos necesarios para que cada usuario guarde la información que crea importante y sobre ella se garantizará la disponibilidad de la información, como mínimo 5 años.
- Todo el software usado en la plataforma tecnológica de Llama.pe debe tener su respectiva licencia y acorde con los derechos de autor.
- Los usuarios deben proteger la información que está contenida en documentos, formatos, listados, etc., los cuales son el resultado de los procesos informáticos; adicionalmente se deben proteger los datos de entrada de estos procesos.
- Los dispositivos electrónicos (computadores, impresoras, multifuncionales, etc.) solo deben utilizarse para los fines autorizados por la empresa.

5.1.7 GESTIÓN DE ACTIVOS

- Los usuarios internos deberán utilizar únicamente los programas y equipos autorizados por la Jefatura de Sistemas.
- La Gerencia o Jefes de áreas deberán proporcionar al usuario interno los equipos informáticos y los programas instalados en ellos; los datos/información creados, almacenados y recibidos, serán propiedad de Llama.pe.
- Los usuarios internos no deben realizar intencionalmente actos que impliquen un mal uso de los recursos tecnológicos. Estos actos incluyen, pero no se limitan a: envió de correo electrónico masivo con fines no institucionales y práctica de juegos en línea.
- El usuario interno deberá informar al Jefe Inmediato de cualquier violación de las Políticas de Seguridad o uso indebido que tenga conocimiento.
- Ningún usuario interno deberá acceder a la red o a los servicios TIC de Llama.pe, utilizando una cuenta de usuario o clave de otro usuario.
- El uso de certificados digitales es exclusivo para los procesos permitidos en llama.pe y autenticación en las plataformas de la misma.
- El acceso a los activos digitales (datos y documentos) son exclusivos para los usuarios con los permisos necesarios.

Los demás puntos se inician en el documento **LLA-CLA-008**

5.1.8 POLÍTICAS DE USO DE INTERNET

- La navegación en Internet debe realizarse de forma razonable y con propósitos laborales.
- No se debe permitir la navegación a sitios con contenidos contrarios a la ley o a las políticas de Llama.pe o que representen peligro para la entidad.
- La descarga de archivos de Internet debe ser con propósitos laborales y de forma razonable para no afectar el servicio de Internet/Intranet.
- Solo en los casos de indisponibilidad prolongada de internet en las oficinas, los trabajadores deberán de usar los datos de los celulares de la empresa para compartir internet a los dispositivos, y comunicar su nueva ip al Administrador del sistema.

Los demás puntos se inician en el documento **LLA-CLA-013**

5.1.9 POLÍTICAS DE USO DE MENSAJERÍA Y REDES SOCIALES

- El uso de servicios de mensajería y el acceso a redes sociales deben ser autorizados solo para un grupo reducido de usuarios, teniendo en cuenta sus funciones y para facilitar canales de comunicación con los clientes.
- No se debe permitir el envío de mensajes con contenido que atente contra la integridad de las personas o instituciones o cualquier contenido que represente riesgo de código malicioso.

Los demás puntos se inician en el documento **LLA-CLA-013**

5.1.10 POLÍTICAS ESPECÍFICAS PARA COLABORADORES Y PROGRAMADORES

- El personal de Sistemas no debe dar a conocer su clave de usuario a terceros.
- El personal de Sistemas debe emplear obligatoriamente las claves o contraseñas con un alto nivel de complejidad y utilizar los servicios de autenticación fuerte que posee la entidad de acuerdo con el rol asignado.
- Para el cambio o retiro de equipos de colaboradores, se deben llevar a cabo mejores prácticas para la eliminación de la información de acuerdo al software disponible en la entidad. Ejemplo:
    - Formateo seguro
    - Destrucción total de documentos
    - Borrado seguro de equipos electrónicos.
- El acceso a cualquier servicio, servidor o sistema de información debe ser autenticado y autorizado.
- Todos los servidores virtuales deben ser configurados con los servicios necesarios y obligatorios para desarrollar las funciones designadas.

5.1.11 POLÍTICAS DE DISPOSICIÓN DE INFORMACIÓN, MEDIOS Y EQUIPOS

Los equipos donde se almacena, procesa o comunica la información, deben mantenerse con las medidas de protección físicas y lógicas, que permitan su monitoreo y correcto estado de funcionamiento; para ello se debe realizar los mantenimientos preventivos y correctivos que se requieran.

Los demás puntos se inician en el documento **LLA-PROC-013**

5.1.12 POLÍTICAS DE RESPALDO Y RESTAURACIÓN DE INFORMACIÓN

- La información de cada sistema debe ser respaldada regularmente sobre un medio de almacenamiento virtual.
- El administrador de los servidores, los sistemas de información o los equipos de comunicaciones, deberá definir o indicar la frecuencia de respaldo y los requerimientos de seguridad de la información (codificación) y también es el responsable de constatar los respaldos periódicos.
- Un procedimiento de contingencia debe ser desarrollado para todas las aplicaciones que manejen información crítica; el dueño de la información debe asegurar que el plan es adecuado, frecuentemente actualizado y periódicamente probado y revisado.

5.1.13 POLÍTICAS DE GESTIÓN DE ACTIVOS DE INFORMACIÓN

5.1.13.1 INVENTARIO DE ACTIVOS DE INFORMACION

Llama.pe deberá mantener un inventario o registro actualizado de sus activos de información, bajo la responsabilidad de cada propietario de información y centralizado por la Jefatura de Sistemas

5.1.13.2 PROPIETARIOS DE LOS ACTIVOS DE INFORMACION

Los propietarios de los activos de información y los administradores de estos activos son los usuarios internos que hacen uso de estos activos o por su cargo son designados responsables de los mismos, así como de los procesos a su cargo, de los sistemas de información o aplicaciones informáticas o infraestructura de tecnología de información y comunicaciones

Los demás puntos se inician en el documento **LLA-CLA-008**

5.2. REVISIÓN DE LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

El encargado de velar por el cumplimiento de las políticas de seguridad de la información dentro de la empresa es el Oficial de Seguridad de la Información, quien conjuntamente con el Comité de seguridad de la Información de la empresa han establecido que las revisiones de las políticas de seguridad de la información se realicen antes de finalizar el mes de Noviembre (en preparación para la revisión del SGSI por el Alta Gerencia)..

Se establecieron estos intervalos por el hecho de ser el tiempo suficiente para encontrar patrones que requieran algún tipo de ajuste.

6 MEJORA CONTINUA

LLAMA.PE gestiona los procesos necesarios para mejorar continuamente la conveniencia, adecuación y eficacia del Sistema de Gestión de Seguridad de la Información a través de Acciones Correctivas y Mejora Continua, de la política y objetivos de seguridad de la información, los resultados de las auditorías internas, acciones correctivas, revisión por la dirección u otra información relevante.

Los propietarios de riesgos se encuentran comprometidos con la mejora de sus procesos y presentan los resultados de las mejoras y reportes de avance; así como los proyectos de mejora al Oficial de Seguridad de la Información.

Los demás puntos se inician en el documento **LLA-PROC-011**