POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

VERSIÓN: V1.2

PUBLICO

OFICIAL

LN-POL-001

PARA: LLAMA.PE | NUBEFACT | MICONTADOR | QUESITO | NUBECONT | POLLERA | YOUPANA | SONQOY

HISTORIAL DE VERSIONES

VERSIÓN	DESCRIPCIÓN	REALIZADO POR	FECHA DE APROBACIÓN	FECHA DE REVISIÓN
V1.2	se actualiza el alcance involucrando mas elementos - se agregan el punto 2.2 y 2.5	LOUIE DIAZ MARTICORENA	2025-06-09	2025-06-25
V1.1	Se disminuye el contenido original, quitando contenido irrelevante (introducción, definiciones, etc). Se agrega detalle sobre IP y ciberseguridad.	LOUIE DIAZ MARTICORENA	2025-05-08	2025-05-30
V1.0	- Versión inicial conjunta	EDWIN VICENTE PAUCAR ONOFRE	2024-07-05	2025-05-05

Documentos de Herencia

- LN-MAN-001 MANUAL SGSI LLAMA-NUBEFACT

Documentos de Referencia

No tiene documentos de referencia.

Tabla de contenido

1 INTRODUCCIÓN Y PROPOSITO

Garantizar la idoneidad, adecuación y eficacia continuas en la dirección de LA EMPRESA y el apoyo a la seguridad de la información de acuerdo con los requisitos del negocio, legales, estatutarios, regulatorios y contractuales.

2 ALCANCE

Esta política de seguridad tendrá un alcance para cubrir lo siguiente:

- Información
- Activos de la información
- Sistemas
- Procesos y sub procesos
- Personal contratado de la empresa
- Terceros

2.1 OBJETIVOS

Los objetivos claves de seguridad de la información que la política busca alcanzar son:

- Reforzar la cultura de seguridad de la información asegurando que los colaboradores reciban capacitaciones periódicas.
- Gestionar adecuadamente los roles y reglas de acceso.
- Conservar, salvaguardar y proteger los activos de información de la empresa.

Los recursos y planes para alcanzar estos objetivos se detallan en el documento:

OBJETIVOS DE SEGURIDAD

2.2 COMPROMISO DE LA ALTA DIRECCIÓN

El representante legal demuestra su compromiso con la implementación del SGSI y de la políticas:

- Estando en la presentación de los documentos necesarios para el buen funcionamiento del SGSI y aprobándolos.
- Comprometiéndose con la mejora continua del SGSI proporcionando recursos (dinerario y no dinerarios), personal y herramientas.
- Participando de las reuniones de comité, auditorias, cierres de ciclo y capacitaciones grupales o masivas.

2.3 ROLES Y RESPONSABILIDADES

- Dirección
- Responsable del SGSI
- Comité de Seguridad de la Información
- Oficial de Cumplimiento
- Responsable de tecnologías de la información
- Representante de Administración de TI
- Responsable de personas
- Representante de operación
- Todos los Colaboradores

Los roles y responsabilidades se deben regir a la LN-POL-007 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN, el Manual de Organización y Funciones, y/o Manual de Equipo Implementador SGSI.

2.4 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 Cumplimiento, 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 en intervalos de 12 meses (anual).

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

Los patrones que requieran ajustes son ocasionados por las siguientes causas:

- Cambios externos en la Empresa.
- Cambios en las políticas de la SUNAT, INDECOPI o Entidades normativas del Estado.
- Cambios internos dentro de la Empresa.
- Incidentes recurrentes, graves que afecten a la Empresa.

2.5 CUMPLIMIENTO DE REQUISITOS LEGALES

- **Constitución Política del Perú**: prevé que los servicios informáticos, computarizados o no, públicos o privados, no suministren información que afecte la intimidad personal y familiar de las personas.
- **Ley 29733, Ley de Protección de Datos Personales**: desarrolla los derechos de los titulares de datos personales, los principios y las condiciones que se deben aplicar en su tratamiento.
- **Decreto Supremo N.º 016-2024-JUS**: El presente Reglamento tiene por objeto establecer disposiciones para la adecuada aplicación de la Ley N.º 29733, Ley de Protección de Datos Personales, en adelante la Ley, a fin de garantizar el derecho fundamental a la protección de datos personales, regulando un adecuado tratamiento por parte de las personas naturales, entidades públicas y las instituciones pertenecientes al sector privado, particularmente, en el entorno digital.
- **Guía de Acreditación de Entidades de Registro (ER):** Procedimientos y criterios que deben cumplir las Entidades de Registro para lograr su acreditación ante el INDECOPI.
- **Obligaciones para ser una OSE**: Implementar los requisitos establecidos por la ISO/IEC-27001 desde el inicio del segundo año de haber inscrito en el Registro OSE.

3. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

3.1 ASEGURAR LA PROTECCIÓN DE DATOS PERSONALES

Esta política es un compromiso con la seguridad de la información y con todos nuestras partes interesadas.

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

1 SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

1. Los niveles de clasificación de la información incluyen: USO INTERNO, PÚBLICO, CONFIDENCIAL y DATOS PERSONALES.
2. Debemos garantizar que la recolección, almacenamiento, tratamiento y eliminación de los datos personales cumpla con la normativa aplicable para proteger los derechos de los titulares.
3. Las aplicaciones y sistemas estarán protegidos contra accesos no autorizados mediante controles de ciberseguridad como firewalls, autenticación multifactor, y monitoreo continuo de vulnerabilidades.
4. Disponer de personal para el monitoreo de activos de información y la atención inmediata a los incidentes y/o eventos de seguridad.

2 GESTIONAR LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

1. El Comité de Seguridad del SGSI de la Empresa se reúne periódicamente para detectar los riesgos de seguridad tomando en cuenta la LN-MET-001 METODOLOGÍA DE GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN para la elaboración y actualización del Inventario de activos, evaluación de riesgos, tratamiento del riesgo y declaración de aplicabilidad.

3 ATENDER DE INMEDIATO CUALQUIER VIOLACIÓN DE SEGURIDAD DE LA INFORMACIÓN DETECTADA EN LA EMPRESA

1. Todo trabajador o usuario interno deberá informar al Jefe Inmediato de cualquier violación de las Políticas de Seguridad o uso indebido que tenga conocimiento, así como las medidas a tomar de acuerdo al LN-PRO-003 PROCEDIMIENTO DE GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION.
2. El personal de sistemas encargado del monitoreo debe revisar los activos críticos de acuerdo al procedimiento LN-PRO-036 MONITOREOS DE EQUIPOS REMOTO, LN-PRO-010 PROCEDIMIENTO PARA REVISAR EQUIPOS DEL PERSONAL.

3.2. Ser uno con el SGSI por medio del aprendizaje continuo

1. **PARTICIPAR EN TODAS LAS CAPACITACIONES DE SEGURIDAD DE LA INFORMACIÓN**
    1. El Oficial de Cumplimiento periódicamente y de acuerdo al LN-PLAN-003 Plan de concientización y capacitación realizará talleres con las distintas áreas de la Empresa.
    2. Todo el personal debe interesarse y participar de estas capacitaciones y evaluaciones.
2. **LEER Y DAR CUMPLIMIENTO A LOS DISTINTOS DOCUMENTOS PROPORCIONADOS POR LA EMPRESA Y CONFIRMAR SU RECEPCIÓN**
    1. Todo el personal debe revisar y poner en práctica las distintas políticas de seguridad, políticas de tópico específico, procedimientos, formatos y documentos que recibe por correo electrónico o por otro medio cada vez que son actualizadas.
3. **CUMPLIR CON RESPONSABILIDAD Y COMPROMISO LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN Y PROTECCIÓN DE LOS ACTIVOS QUE ME ASIGNE LA EMPRESA.**
    1. Los líderes de círculo deben asegurarse que todos los procedimientos de seguridad de la información dentro de su círculo, se comuniquen, realicen, y monitoreen correctamente para lograr el cumplimiento de las políticas y estándares de seguridad de la información de la Empresa.
    2. El Comité de Seguridad del SGSI de la Empresa debe identificar los riesgos a los que está expuesta la información de las distintas áreas, teniendo en cuenta que la información pueda ser copiada, divulgada, modificada o destruida física o digitalmente por personal interno o externo.
    3. Se debe asegurar que los líderes de círculo, terceros, trabajadores y colaboradores de la Empresa, entiendan sus responsabilidades en relación con las políticas de seguridad de la información de la Empresa y actúen de manera consistente frente a las mismas, con el fin de reducir el riesgo de hurto, fraude, filtraciones o uso inadecuado de la información o los equipos empleados para el tratamiento de la información.
    4. Los usuarios internos deberán utilizar únicamente los programas y equipos autorizados por el líder de círculo de Sistemas.
    5. La Gerencia o Jefe de Sistemas deberán proporcionar al usuario interno los equipos informáticos y los programas instalados en ellos; los datos/información creados, almacenados y recibidos, serán propiedad de la Empresa.

3.3. INFORMAR, MEDIR Y MEJORA CONTINUA

1. **ACTUALIZAR Y MEJORAR CONSTANTEMENTE EL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI)**
    1. La Gerencia debe diseñar, programar y realizar los programas de auditoría del sistema de gestión de seguridad de la información.
    2. La Empresa deberá mantener un inventario o registro actualizado de sus activos de información, bajo la responsabilidad de cada propietario de información y centralizado por el líder de círculo de Sistemas.
    3. La documentación actualizada es distribuida al personal previa autorización del Comité de Seguridad.
2. **REALIZAR Y PROMOVER EVALUACIONES, MANTENIMIENTOS Y PRUEBAS PERIÓDICAS**
    1. El Líder de Sistemas en coordinación con el Oficial de Seguridad deberán definir o indicar la frecuencia de respaldo y los requerimientos de seguridad de la información (codificación).
    2. El Jefe de Sistemas es el responsable de constatar los respaldos periódicos.
    3. Para ello el círculo de sistemas debe tomar en cuenta el Plan de Recuperación de Desastres.

4. POLÍTICAS DE TÓPICO ESPECÍFICO

POLÍTICA	FINALIDAD
LN-POL-002 GESTIÓN DE ACTIVOS	Establece los lineamientos para la identificación, valoración y protección de los activos de información.
LN-POL-003 CONTROL DE ACCESO	Establece los controles necesarios para acceder a las plataformas, aplicaciones e información que ellos contengan.
LN-POL-004 POLÍTICA DE SEGURIDAD FÍSICA Y AMBIENTAL	Establece las medidas para crear ambientes y áreas seguras de la empresa.
LN-POL-005 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN	Establece los requisitos/obligaciones que se deben aplicar al adquirir, desarrollar y/o mantener sistemas de información internos o de terceros.
LN-POL-006 POLÍTICA DE RELACIÓN CON PROVEEDORES	Determina los requisitos obligatorios para con los proveedores.
LN-POL-007 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	Determina los roles y responsabilidad que tiene cada uno en el Sistema de Gestión de Seguridad de la Información.
LN-POL-008 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	Establece las medidas a tomar en caso se presente una incidencia de seguridad.
LN-POL-009 SEGURIDAD DE LOS RECURSOS HUMANOS	Establece lo lineamientos para garantizar que el personal sea consciente y se comprometa con el cumplimiento de las políticas y procedimientos.
LN-POL-010 POLÍTICA DE CRIPTOGRAFÍA	Determina los lineamientos para asegurar el uso adecuado de criptografía para proteger la información en aspectos de confidencialidad e integridad.
LN-POL-011 POLÍTICA DE CUMPLIMIENTO	Establece los lineamientos para determinar y cumplir los requerimientos, y prevenir infracciones de las obligaciones legales.
LN-POL-012 SEGURIDAD EN LAS OPERACIONES	Establece las medidas para garantizar el funcionamiento correcto de las operaciones críticas.
LN-POL-013 GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	Determina las acciones a realizar para planificar y probar los Planes de Recuperación de Desastres.
LN-POL-014 POLÍTICA DE TRANSFERENCIA DE INFORMACIÓN	Establece los criterios para la transferencia de información entre sistemas, usuarios internos y usuarios externos.