



Universidad
Nacional
de Loja

Dirección de
Tecnologías de Información

[POLÍTICA]

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Versión 26.08

Agosto 2026

Educamos para **Transformar**



HISTORIAL DE CAMBIOS

Versión	Fecha	Responsable	Descripción de la modificación
26.08	13/08/2026	Ing. Juan Carlos Riofrío Herrera	Documento inicial



Universidad
Nacional
de Loja

Dirección de
Tecnologías de Información

CONTENIDOS

1. Antecedentes	4
2. Objetivo de la política	4
3. Política de seguridad de la información	5
3.1. Descripción de la Política	5
3.2. Declaración de los objetivos de seguridad de la información	5
3.3. Roles y Responsabilidades	6
3.3.1. Máxima Autoridad (Rector)	6
3.3.2. Comité de Seguridad de la Información (CSI)	7
3.3.3. Oficial de Seguridad de la Información (OSI)	7
3.3.4. Responsables de activos de información	7
3.3.5. Dirección de Tecnologías de Información	7
3.3.6. Comunidad universitaria y usuarios externos	8
3.4. Alcance y usuarios	8
3.5. Comunicación de la política	9
3.6. Excepciones y sanciones	9
3.6.1. Excepciones	9
3.6.2. Sanciones	10
4. Glosario de términos	10
5. Documentos de Referencia	11
6. Firmas de responsabilidad	12

1. Antecedentes

La información es uno de los activos de mayor valor para la Universidad Nacional de Loja, siendo un elemento fundamental para el cumplimiento de sus objetivos estratégicos de docencia, investigación y vinculación con la sociedad. En un entorno de creciente interconexión, impulsado por los avances tecnológicos, surgen de manera constante nuevas amenazas que ponen en riesgo la seguridad de la información. Por esta razón, se requiere la implementación de mecanismos formales que garanticen su adecuada protección.

Diversas normativas de carácter regulatorio exigen a las instituciones públicas la adopción de medidas para salvaguardar la información. Entre las más relevantes se encuentran la Constitución de la República, la Ley Orgánica de Protección de Datos Personales y su Reglamento, el Esquema Gubernamental de Seguridad de la Información (EGSI) emitido por el Ministerio de Telecomunicaciones y de la Sociedad de la Información, y las Normas de Control Interno de la Contraloría General del Estado. Este marco legal establece la obligatoriedad de implementar sistemas de gestión y controles para proteger los datos personales y la información institucional.

En este contexto, la presente Política de Seguridad de la Información se establece como el documento de más alto nivel que direcciona la gestión de la seguridad en la Universidad Nacional de Loja. Su propósito es definir el objetivo, la dirección, los principios y las reglas básicas para proteger los activos de información, garantizando su confidencialidad, integridad y disponibilidad. Este documento refleja el compromiso de la máxima autoridad de la institución con la implementación, mantenimiento y mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI), basado en el EGSI y en buenas prácticas reconocidas, con el fin de prevenir y mitigar los riesgos que puedan afectar a la comunidad universitaria y al cumplimiento de los fines institucionales.

2. Objetivo de la política

Establecer el marco de actuación y los lineamientos generales para la gestión de la seguridad de la información en la Universidad Nacional de Loja protegiendo los activos de información de la institución, asegurando su confidencialidad, integridad y disponibilidad, independientemente del formato en que se encuentren.

Asimismo, esta política busca dirigir y soportar la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) que permita conocer, gestionar y minimizar los riesgos a los que está expuesta la información. Esto se logrará mediante la definición de políticas, normas y directrices alineadas al marco legal vigente y a estándares de buenas prácticas, que guíen el tratamiento de la

información durante todo su ciclo de vida: desde su creación hasta su destrucción final.

3. Política de seguridad de la información

3.1. Descripción de la Política

La máxima autoridad y el Comité de Seguridad de la Información de la Universidad Nacional de Loja, en reconocimiento de la importancia de la información como un activo estratégico, se comprometen con la implementación, operación y mejora continua de un Sistema de Gestión de Seguridad de la Información (SGSI). Este sistema busca establecer un marco de confianza en el ejercicio de las funciones académicas, de investigación y de vinculación, en estricto cumplimiento del marco legal vigente y en plena concordancia con la misión y visión institucionales.

Para la Universidad Nacional de Loja, la protección de la información tiene como finalidad la reducción del impacto generado sobre sus activos por los riesgos identificados de manera sistemática. El objetivo es mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de la misma, acorde con las necesidades de la comunidad universitaria y los diferentes grupos de interés.

En consecuencia, esta política es de aplicación y cumplimiento obligatorio para toda la institución. Incluye a todo el personal, como estudiantes, docentes, administrativos y trabajadores; así como a terceros que, en el ejercicio de sus funciones o prestación de servicios, tengan acceso, generen, procesen o custodien información propiedad de la Universidad Nacional de Loja o bajo su responsabilidad.

3.2. Declaración de los objetivos de seguridad de la información

La Universidad Nacional de Loja establece los siguientes objetivos de seguridad de la información, los cuales se encuentran directamente alineados con los Objetivos Estratégicos (OE) definidos en el PEDI 2024-2028, con el propósito de garantizar la protección de los activos de información, minimizar los riesgos asociados y fortalecer la gestión de seguridad en la institución:

- **Objetivo 1: Fortalecer la cultura de seguridad de la información y el cumplimiento normativo.** Este objetivo se encuentra alineado al OE 4. Busca promover una cultura organizacional donde la seguridad sea una responsabilidad compartida, mediante la

capacitación y sensibilización continua de la comunidad universitaria, asegurando la correcta aplicación de los lineamientos del ECSI y el cumplimiento del marco legal vigente.

- **Objetivo 2: Salvaguardar la información institucional.** Objetivo alineado al OE 2. Busca proteger la confidencialidad, integridad y disponibilidad de la información, propiedad o bajo responsabilidad de la UNL asegurando que estén debidamente resguardados mediante el establecimiento de un conjunto de políticas y directrices, con el fin de conocer, gestionar y minimizar los riesgos de seguridad.
- **Objetivo 3: Gestionar los riesgos de seguridad para fortalecer la gestión institucional.** Este objetivo se encuentra alineado al OE 4. Busca implementar un proceso continuo de gestión de riesgos de seguridad de la información, mediante la identificación, evaluación y mitigación de amenazas, asegurando la aplicación de controles adecuados y alineados con los lineamientos del ECSI para proteger los procesos institucionales.
- **Objetivo 4: Fortalecer la resiliencia operativa y la continuidad de los servicios académicos.** Alineado al OE 1, y OEI 4. Busca incrementar la efectividad operacional de los procesos y servicios críticos, implementando planes de continuidad y recuperación ante desastres que permitan garantizar la disponibilidad de los servicios académicos y administrativos ante fallas tecnológicas, ciberataques o eventos de fuerza mayor.

3.3. Roles y Responsabilidades

Para garantizar la adecuada gestión y protección de los activos de información de la Universidad Nacional de Loja, se establecen los siguientes roles y responsabilidades, los cuales son de cumplimiento obligatorio para toda la comunidad universitaria.

3.3.1. Máxima Autoridad (Rector)

El Rector, como máxima autoridad y representante legal de la Universidad Nacional de Loja, conforme se indica en el ACUERDO Nro. MINTEL-MINTEL-2024-0003, en sus Art. 5 y 6, es el principal responsable de impulsar y respaldar la seguridad de la información en la institución, aprobando la política de seguridad de la información y demás documentación que requiera este nivel de aprobación, así como asignar los recursos necesarios.

3.3.2. Comité de Seguridad de la Información (CSI)

Es el organismo encargado de la planificación, supervisión y seguimiento de las estrategias de seguridad de la información en la institución. Sus principales responsabilidades se encuentran descritas en el “REGLAMENTO PARA EL FUNCIONAMIENTO DEL COMITÉ DE SEGURIDAD DE LA INFORMACIÓN DE LA UNIVERSIDAD NACIONAL DE LOJA”.

3.3.3. Oficial de Seguridad de la Información (OSI)

Es el responsable de la gestión operativa y la coordinación de la implementación del SGSI en la institución, asesorando al CSI y a las demás unidades. Sus funciones principales son las descritas en el “ACUERDO Nro. MINTEL-MINTEL-2024-0003”.

3.3.4. Responsables de activos de información

Los responsables de los procesos gobernantes, agregadores de valor, habilitantes y de apoyo son considerados los máximos responsables de los activos de información bajo su gestión. Sus responsabilidades son:

- Clasificar la información generada y administrada en sus respectivas unidades.
- Garantizar que el personal a su cargo conozca y cumpla con la presente política y las normativas de seguridad.
- Colaborar con el OSI en el proceso de análisis de riesgos de sus activos de información y en la implementación de los controles requeridos.
- Autorizar el acceso a la información de su competencia, aplicando el principio de mínimo privilegio y normativa aplicable.

3.3.5. Dirección de Tecnologías de Información

La Dirección de Tecnologías de Información es responsable de la implementación, gestión y mantenimiento de los controles técnicos de seguridad de la información en la infraestructura tecnológica y sistemas informáticos de la UNL. Sus responsabilidades incluyen:

- Administrar los controles de acceso lógico a los sistemas informáticos, redes y aplicaciones, de acuerdo con las autorizaciones de los responsables de los activos.
- Implementar y gestionar los mecanismos de respaldo y recuperación de la información institucional.
- Monitorear la infraestructura tecnológica para detectar y prevenir actividades anómalas o incidentes de seguridad.

- Garantizar la correcta configuración de seguridad de los sistemas informáticos, la actualización de software y la aplicación de parches de seguridad para mitigar las vulnerabilidades.
- Proveer la gestión servicios tecnológicos necesarios durante la gestión y resolución de incidentes de seguridad.

3.3.6. Comunidad universitaria y usuarios externos

Todos los miembros de la comunidad universitaria, así como usuarios externos con acceso a los activos de información de la UNL, tienen la obligación de:

- Conocer y cumplir con lo establecido en la presente Política de Seguridad de la Información y las normativas que de ella se deriven.
- Manejar la información de manera responsable, protegiendo su confidencialidad, integridad y disponibilidad en el desarrollo de sus actividades diarias.
- Reportar de forma inmediata al canal correspondiente cualquier evento, incidente o vulnerabilidad de seguridad que identifiquen.
- Participar activamente en los programas de capacitación y concienciación en seguridad de la información que la institución organice.
- Proteger las credenciales de acceso (usuarios y contraseñas) asignadas, las cuales son de uso personal e intransferible.

3.4. Alcance y usuarios

3.4.1. Alcance

La presente Política de Seguridad de la Información establece los lineamientos generales, objetivos, roles y responsabilidades para garantizar la adecuada protección de todos los activos de información de la Universidad Nacional de Loja. Su alcance abarca toda la información, independientemente del medio en que se encuentre (digital, físico u otro), así como los sistemas informáticos, redes, plataformas tecnológicas y los procesos institucionales (gobernantes, agregadores de valor, habilitantes y de apoyo) que la generan, procesan, almacenan o transmiten.

Esta política es de aplicación y cumplimiento obligatorio en el marco del Esquema Gubernamental de Seguridad de la Información (EGSI), y su implementación es supervisada por el Comité de Seguridad de la Información (CSI) de la UNL.

3.4.2. Usuarios

Son usuarios de esta política todas las personas y entidades que, por la naturaleza de sus funciones o relación con la institución, interactúan con los activos de información de la Universidad Nacional de Loja. Se incluyen los siguientes:

- Autoridades, docentes, administrativos y trabajadores de la UNL.
- Estudiantes y alumni
- Contratistas, proveedores, consultores y personal externo que presten o usen servicios de la institución.
- Terceros o entidades externas que accedan a información de la UNL en virtud de convenios, acuerdos de cooperación u otros instrumentos legales.

El cumplimiento de esta política, y su normativa secundaria es de carácter obligatorio para todos los usuarios mencionados, quienes deben acatar sus disposiciones y contribuir activamente a la protección de la información en la Universidad.

3.5. Comunicación de la política

La Política de Seguridad de la Información y sus políticas específicas serán difundida de manera obligatoria y sistemática a todos los miembros de la comunidad universitaria, así como a contratistas y terceros con acceso a la información institucional a través de los canales y medios establecidos, garantizando su comprensión y aplicación en todos los niveles de la institución.

3.6. Excepciones y sanciones

3.6.1. Excepciones

La presente Política de Seguridad de la Información y sus políticas específicas son de aplicación y cumplimiento obligatorio para todos los usuarios definidos en el alcance. Sin embargo, podrán existir excepciones que se encuentren determinadas en la ley.

Cualquier excepción deberá ser aprobada por el Comité de Seguridad de la Información (CSI) y documentada formalmente, asegurando que no comprometa la confidencialidad, integridad y disponibilidad de la información institucional.

3.6.2. Sanciones

El incumplimiento de las disposiciones establecidas en esta política y en las políticas específicas que de ella se deriven, será considerado una falta y dará lugar a la aplicación de las medidas disciplinarias correspondientes. Toda inobservancia será sancionada de conformidad con las leyes y reglamentos vigentes.

4. Glosario de términos

Término	Definición
Política de Seguridad de la Información	Documento de más alto nivel que direcciona la gestión de la seguridad, definiendo el objetivo, los principios y las reglas básicas para proteger los activos de información de la Universidad.
Activos de Información	Cualquier recurso de valor para la Universidad que contiene o procesa información. Incluye no solo los datos (digitales o físicos), sino también los sistemas, las aplicaciones, las redes, la infraestructura tecnológica y el conocimiento de las personas. Ejemplos: las calificaciones de los estudiantes, los datos de una investigación, el sistema académico, una base de datos.
Continuidad	Capacidad de la Universidad para mantener la disponibilidad de sus procesos y servicios críticos, especialmente los académicos, ante fallas o eventos de fuerza mayor.
Comité de Seguridad de la Información (CSI)	Organismo institucional encargado de la planificación, supervisión y seguimiento de las estrategias de seguridad de la información.
Control	Medida de seguridad, ya sea administrativa, técnica u organizativa, implementada para mitigar los riesgos identificados.
Esquema Gubernamental de Seguridad de la Información (EGSI)	Marco normativo emitido por el Ministerio de Telecomunicaciones y de la Sociedad de la Información, de cumplimiento obligatorio para las instituciones públicas del Ecuador.

Integridad	Propiedad que salvaguarda la exactitud y completitud de la información, protegiéndola de modificaciones no autorizadas.
Oficial de Seguridad de la Información (OSI)	Responsable de la gestión operativa y la coordinación de la implementación del Sistema de Gestión de Seguridad de la Información (SGSI) en la institución.
Riesgo	Posibilidad de que una amenaza explote una vulnerabilidad, causando un impacto adverso en los activos de información y en el cumplimiento de los objetivos institucionales.
Sistema de Gestión de Seguridad de la Información (SGSI)	Enfoque sistemático basado en el EGSi para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información en la Universidad.

5. Documentos de Referencia

Esta política se fundamenta en un conjunto de normativas, estándares y documentos internos que definen el marco de trabajo para la seguridad de la información en la Universidad Nacional de Loja. Los documentos de referencia clave son:

- Ley Orgánica de Protección de Datos Personales y su Reglamento.
- Normas de Control del Sector Público y Jurídicas de Derecho Privado.
- Acuerdo Ministerial 2024-003.
- Esquema Gubernamental de Seguridad de la Información (EGSI v3.0)
- Normas Técnicas Ecuatorianas NTE INEN-ISO/IEC 27001, NTE INEN-ISO/IEC 27002, NTE INEN-ISO/IEC 27005
- Plan Estratégico de Desarrollo Institucional 2024-2028
- Reglamento Interno del Comité de Seguridad de la Información (CSI-UNL)
- Plan de Implementación del Esquema Gubernamental de Seguridad de la Información (EGSI v3) en la Universidad Nacional de Loja.
- Plan de Comunicación y Sensibilización (EGSI v3).

6. Firmas de responsabilidad

Acción	Funcionario	Firma
Elaborado por:	Ing. Juan Carlos Riofrío Herrera OFICIAL DE SEGURIDAD DE LA INFORMACIÓN (OSI)	 Validar únicamente en FirmaEC. Firmado electrónicamente por: JUAN CARLOS RIOFRIO HERRERA
Revisado por:	Ing. Jhon Alexander Calderón Sanmartín DIRECTOR DE TECNOLOGÍAS DE LA INFORMACIÓN	 Validar únicamente en FirmaEC. Firmado electrónicamente por: JHON ALEXANDER CALDERON SANMARTIN
Aprobado: *Comité de Seguridad de la Información (CSI-UNL)	Ing. Magda Cecilia Salazar González DIRECTORA DE PLANIFICACIÓN Y DESARROLLO	 Validar únicamente en FirmaEC. Firmado electrónicamente por: MAGDA CECILIA SALAZAR GONZALEZ

* En nombre del Comité de Seguridad de la Información, suscribe la Presidenta.