



Universidad
Nacional
de Loja

Dirección de
Tecnologías de Información

[POLÍTICA]

POLÍTICA DE SISTEMAS INFORMÁTICOS INSTITUCIONALES

Versión 26.08

Agosto 2026

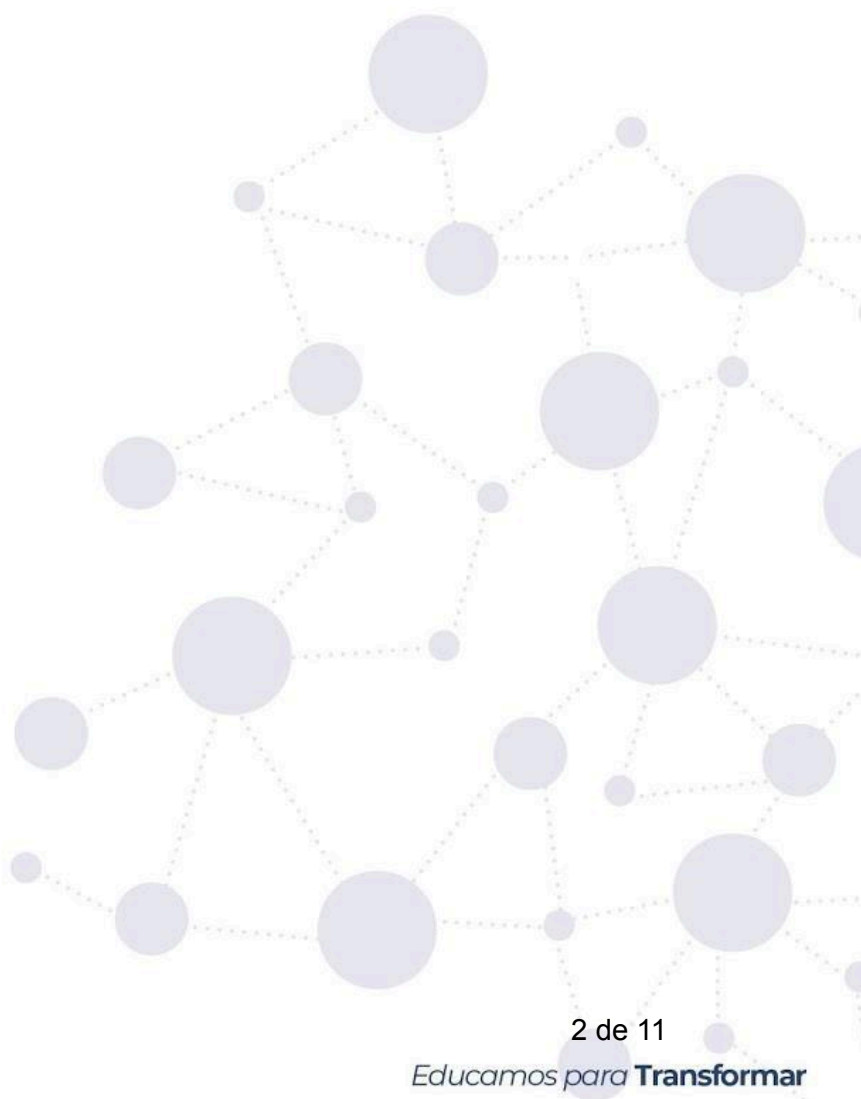
1 de 11

Educamos para **Transformar**



HISTORIAL DE CAMBIOS

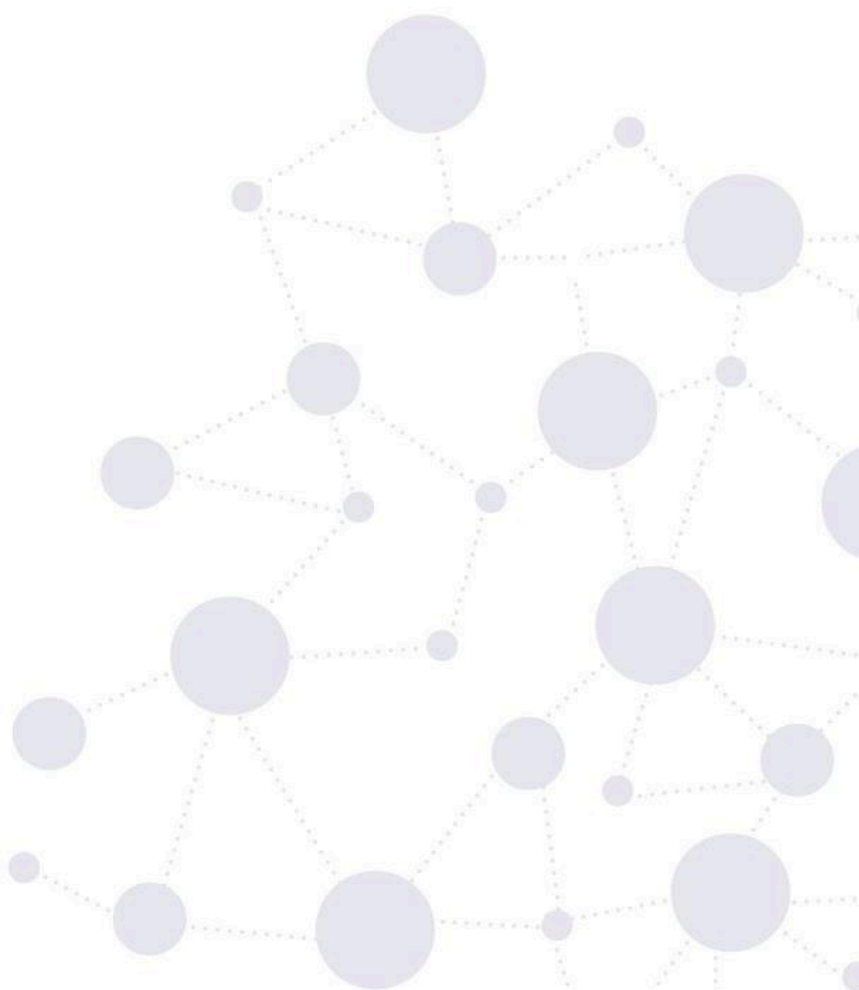
Versión	Fecha	Responsable	Descripción de la modificación
26.08	13/08/2026	Ing. Juan Carlos Riofrío Herrera	Documento inicial





CONTENIDOS

1. Objetivo	4
2. Alcance	4
3. Política	4
4. Lineamientos de la política	4
4.1. Desarrollo de software interno	4
4.2. Mantenimiento de software	7
4.3. Interoperabilidad con servicios gubernamentales	7
4.4. Validez y gestión del documento	8
5. Glosario de términos	8
6. Documentos de Referencia	10
7. Firmas de responsabilidad	11



1. Objetivo

Establecer las directrices formales, procedimentales y técnicas orientadas a integrar la seguridad de la información en todas las fases de conceptualización, desarrollo, adquisición y mantenimiento de software, priorizando el uso de software libre y protegiendo los activos de información de la Universidad Nacional de Loja (UNL).

2. Alcance

Esta política es de cumplimiento obligatorio para la comunidad universitaria y terceros, conforme a los alcances y usuarios definidos en la Política de Seguridad de la Información, que participen en el análisis, codificación, implantación, contratación o soporte de cualquier sistema informático que procese información de la UNL o se aloje en su infraestructura tecnológica.

3. Política

La Universidad Nacional de Loja se compromete a implementar controles de seguridad desde el diseño y por defecto en todo su ecosistema de software, alineados al Esquema Gubernamental de Seguridad de la Información (EGSI v3), la Ley Orgánica de Protección de Datos Personales (LOPD), y las mejores prácticas internacionales, priorizando el uso de tecnologías de código abierto.

4. Lineamientos de la política

4.1. Desarrollo de software interno

La ciberseguridad y la protección de datos personales se integrarán en todas las fases del ciclo de vida del software, desde la planificación estratégica hasta su retiro definitivo. Todo proyecto de desarrollo deberá estar alineado al Plan Estratégico de Desarrollo Institucional (PEDI) y formar parte del Plan de Desarrollo de Software aprobado por la Dirección de Tecnologías de Información (DTI).

Antes de iniciar la etapa de construcción, los requerimientos de ciberseguridad deberán definirse y documentarse formalmente para su validación por parte de la Dirección de Tecnologías de Información (DTI).

Todo el código fuente, arquitecturas, documentación técnica y artefactos generados por el personal de la DTI, así como por estudiantes en proyectos de titulación o pasantías, constituyen propiedad intelectual y patrimonial exclusiva de la UNL.

Los sistemas informáticos de la UNL que requieran autenticación deberán integrarse de manera obligatoria al Servicio de Autenticación Centralizada (SSO + 2FA). Asimismo, los sistemas informáticos deberán soportar la revocación

inmediata de accesos y contar con mecanismos de cierre de sesión automático por inactividad.

La gestión de accesos, que comprende la creación y administración de cuentas de usuarios, la asignación de roles y la definición de privilegios dentro de los sistemas informáticos, deberá alinearse estrictamente a la "Política de Control de Acceso Lógico".

Los diseños arquitectónicos se basarán en los principios de "Seguridad desde el diseño" y "Confianza Cero (Zero Trust)", asumiendo que ninguna red o usuario es confiable por defecto. En consecuencia, se integrarán prácticas de codificación segura para mitigar vulnerabilidades desde el origen del ciclo de vida del software.

El desarrollo de software se gestionará bajo el Marco de Trabajo de Desarrollo de Software de la DTI, el mismo que debe contemplar de manera secuencial: la formulación del requerimiento, la elaboración del perfil de proyecto (que incluirá el estudio de factibilidad), la refinación y priorización de los requerimientos, la implementación (construcción), y las fases de revisión y retrospectiva (mediante pruebas piloto o demostraciones). Finalmente, el lanzamiento y puesta en producción requerirá la elaboración previa de toda la documentación habilitante correspondiente; para el caso de software nuevo, se incluirá obligatoriamente una etapa posterior de monitoreo.

El equipo técnico respetará la Guía de Desarrollo de Software vigente para estandarizar lenguajes, estructuras de proyectos, frameworks y entornos autorizados.

Previo al lanzamiento final en producción, además de la certificación técnica de control de calidad, el sistema deberá contar el Acta de Paso a Producción revisada y/o legalizada por la unidad requirente, garantizando que la solución satisface las necesidades funcionales aprobadas.

De manera transversal, se debe contar con un plan de contingencia. Este servirá como guía de acción para restaurar los sistemas y ejecutar el retorno (rollback) de configuraciones ante cualquier fallo, caída o eventualidad técnica que comprometa la estabilidad del servicio.

Los ambientes de desarrollo, pruebas (QA) y producción deben operar bajo esquemas de separación lógica o administrativa que prevengan la afectación cruzada e interferencia entre ellos. Se emplearán credenciales de administración independientes para cada entorno, respetando los principios de mínimo privilegio. El acceso a estos ambientes estará estrictamente limitado al personal autorizado según sus funciones.

Todo desarrollo propio debe incorporar prácticas de codificación para mitigar vulnerabilidades comunes, pero no limitadas a:

- Prevención de inyección de código mediante el tratamiento adecuado de parámetros de consulta.
- Controles de acceso robustos basados en roles.
- Gestión y actualización constante de dependencias y librerías para evitar componentes obsoletos.
- Implementación de algoritmos de cifrado fuertes y protección de datos sensibles en reposo y tránsito.

Todo el código institucional debe almacenarse en repositorios centralizados bajo el control estricto de la DTI. Se deben proteger obligatoriamente las ramas principales (master) de los proyectos contra su eliminación, quedando estrictamente prohibida la publicación o integración directa de modificaciones en el código principal.

Para garantizar la integridad y trazabilidad de los sistemas informáticos, todo desarrollo y modificación de software deberá gestionarse mediante un sistema de control de versiones centralizado. Cada iteración o cambio en el código fuente deberá registrarse detallando el autor, la fecha y la descripción de la modificación. Además, es mandatorio que el código fuente esté estructurado y comentado para asegurar su comprensión y facilitar el mantenimiento a largo plazo.

El personal técnico encargado de realizar el paso a producción es responsable de trasladar el software de forma segura al entorno real, validando que los cambios cuenten con las aprobaciones formales y hayan superado las pruebas de control de calidad previas. Durante el paso a producción, el encargado deberá ejecutar la implementación, monitorear el correcto funcionamiento del sistema inmediatamente tras el lanzamiento y, en caso de fallos, gestionar el plan de contingencia.

Cada publicación o actualización de los sistemas deberá documentarse, detallando los cambios realizados junto con su número de versión y fecha correspondiente.

Queda estrictamente prohibido utilizar bases de datos con información real en ambientes de desarrollo o pruebas. Los desarrolladores deberán generar datos sintéticos u ofuscar/anonimizar los registros antes de usarlos. Las excepciones pueden ser autorizadas solamente por el Delegado de Protección de Datos Personales, en cuyo caso, el Especialista de Sistemas Información debe definir cómo se protegerán esos datos de prueba.

Previo el paso a producción de nuevos desarrollos, módulos o modificaciones significativas, el software deberá someterse obligatoriamente a pruebas de seguridad (como escaneo de código o análisis de vulnerabilidades) en el entorno

de pruebas. Para el caso de cambios menores, ajustes operativos o modificaciones de bajo riesgo (como la actualización de parámetros simples), este requerimiento podrá omitirse o simplificarse, a fin de no afectar la agilidad operativa de los servicios.

Para garantizar la seguridad al trabajar desde equipos personales o redes públicas, no se debe confiar en los controles de seguridad locales del dispositivo. Todo el tráfico y acceso a los recursos de la institución (intranet, servidores y entornos de prueba) debe estar protegido y canalizado mediante una Red Privada Virtual (VPN).

4.2. Mantenimiento de software

Se mantendrá un inventario actualizado de los sistemas informáticos institucionales, registrando para cada uno: componentes de software implementados, bibliotecas/dependencias, servicios activos y puertos de red habilitados.

Se deben ejecutar evaluaciones técnicas periódicas sobre los aplicativos de cara a Internet para aplicar los parches correspondientes que mitiguen riesgos cibernéticos.

Toda aplicación académica, administrativa o plataforma virtual deberá contar con certificados digitales vigentes (SSL/TLS) para garantizar la transmisión cifrada de la información.

Es obligatorio que todo nuevo desarrollo de software incorpore controles de auditoría en sus modelos de datos. Como estándar mínimo, el software debe registrar de forma automática el usuario y la marca de tiempo de cada creación y modificación. En componentes identificados como prioritarios o de alto impacto, la auditoría debe extenderse al registro detallado del campo modificado. Los sistemas heredados o preexistentes se adaptarán a esta norma de manera progresiva conforme sean objeto de refactorizaciones o actualizaciones mayores.

4.3. Interoperabilidad con servicios gubernamentales

Todo nuevo desarrollo de software interno o adquisición de soluciones tecnológicas que requiera la validación de identidad o datos de ciudadanos, deberá contemplar la integración y consumo de los servicios de interoperabilidad del Estado ecuatoriano, a fin de optimizar los trámites institucionales y evitar la solicitud de requisitos documentales físicos.

Las conexiones técnicas hacia el Bus Nacional de Datos o plataformas gubernamentales similares deberán efectuarse bajo los procedimientos establecidos por la entidad gubernamental.

Los sistemas informáticos de la UNL que consuman información de plataformas o servicios gubernamentales deberán garantizar el principio de minimización de datos y el cumplimiento estricto de la Ley Orgánica de Protección de Datos Personales (LOPD). La información consultada se usará exclusivamente para el fin específico del trámite autorizado y queda estrictamente prohibido su almacenamiento persistente o replicación en bases de datos locales, salvo que exista una base legal o el consentimiento explícito del titular que lo justifique.

4.4. Validez y gestión del documento

Este documento entra en vigencia a partir de la fecha de su aprobación por la máxima autoridad de la Universidad Nacional de Loja. Su revisión y actualización periódica se llevarán a cabo al menos una vez cada dos años, o cuando se produzcan cambios legales o tecnológicos significativos.

5. Glosario de términos

Término	Definición
Ciclo de vida del software	Fases secuenciales por las que pasa un sistema o aplicación desde su concepción y planificación inicial, abarcando el diseño, desarrollo, pruebas, despliegue, operación, mantenimiento y, finalmente, su retiro.
Seguridad desde el diseño	Enfoque de ingeniería donde los controles y requisitos de seguridad se integran de forma proactiva y obligatoria desde la primera fase de arquitectura de un proyecto, en lugar de añadirse como un parche al final del desarrollo.
Confianza Cero (Zero Trust)	Modelo estratégico de ciberseguridad que elimina la confianza implícita. Asume que ninguna red, usuario o dispositivo (sea interno o externo) es seguro por defecto, exigiendo una verificación y autenticación continua para cada solicitud de acceso.
Codificación segura	Práctica de escribir el código fuente de los aplicativos aplicando estándares internacionales (como OWASP) y metodologías que previenen vulnerabilidades, minimizando la posibilidad de ataques como inyecciones SQL o escalamiento de privilegios.
Paso a producción	Acción formal y técnica mediante la cual un nuevo software, actualización o modificación abandona los entornos aislados de desarrollo o pruebas, y se implementa en el entorno real y en vivo, quedando disponible para los usuarios finales.

Plan de contingencia o retorno (rollback)	Procedimiento documentado y estructurado que permite revertir un sistema a su última versión estable o estado funcional anterior, en caso de que una actualización, cambio o paso a producción falle o introduzca errores críticos.
Repositorios centralizados	Sistemas de control de versiones (como Git) gestionados institucionalmente, donde se almacena, protege y audita todo el historial del código fuente de los proyectos de software, evitando la fragmentación de la información.
Ofuscar/anonimizar	Proceso técnico que consiste en enmascarar, alterar o eliminar de forma irreversible datos reales (especialmente información personal o sensible) para que puedan ser utilizados de forma segura en entornos de desarrollo o pruebas sin violar la privacidad.
VPN (Red Privada Virtual)	Es un "túnel privado y blindado" en internet. Sirve para que la comunidad universitaria o el personal autorizado pueda conectarse a los sistemas internos e infraestructura de la UNL desde una ubicación externa a la universidad, de forma que nadie más en internet pueda espiar o robar la información que se transmite.
Infraestructura código abierto	Arquitectura y componentes tecnológicos base (como sistemas operativos Linux, servidores web, bases de datos y herramientas de red) construidos con software cuyo código fuente es público y libre. Su adopción garantiza mayor transparencia, facilita las auditorías técnicas de seguridad y evita la dependencia exclusiva de proveedores comerciales, optimizando así los recursos tecnológicos institucionales.
Ciberseguridad	Son todas las acciones, herramientas y buenas prácticas que se usan para proteger hardware, software, redes y los datos de la universidad contra ataques de hackers, robos, daños o virus informáticos.
Hardening	Proceso de fortalecimiento de la seguridad de un servidor, sistema operativo o red, cuyo objetivo es reducir su superficie de ataque mediante la eliminación de servicios innecesarios, cierre de puertos inactivos y la configuración estricta de políticas.
Riesgo Cibernético	Probabilidad de que una amenaza explote vulnerabilidades en los activos de información, sistemas operativos, infraestructura tecnológica o procesos, generando un impacto negativo en la confidencialidad, integridad o disponibilidad de la información institucional.
Software libre	Programas informáticos que otorgan a los usuarios y a la institución la libertad fundamental de ejecutar, copiar, distribuir, estudiar, modificar y mejorar el código fuente. Su

	adopción promueve la soberanía tecnológica, evita el pago innecesario de licencias comerciales y fomenta el desarrollo colaborativo, alineándose con los objetivos de optimización de recursos del Estado.
Interoperabilidad	Capacidad de los sistemas de información y de los procedimientos a los que éstos dan soporte, de compartir datos y posibilitar el intercambio de información y conocimiento entre ellos de forma segura y estandarizada.

6. 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 cuales se listan a continuación:

- Ley Orgánica de Protección de Datos Personales (Capítulo 6)
- Normas de Control del Sector Público y Jurídicas de Derecho Privado. (410-11)
- Acuerdo Ministerial 2024-003. Esquema Gubernamental de Seguridad de la Información (EGSI v3.0), ítems 4.4, 4.25, 4.26, 4.27, 4.28, 4.29, 4.30, 4.31, 4.32.
- 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
- Plan de Implementación del Esquema Gubernamental de Seguridad de la Información (EGSI v3) en la Universidad Nacional de Loja.
- Política de Seguridad de la Información.
- Instructivo Normativo Interno de Protección de Datos Personales de la UNL (RESOLUCIÓN N° 062-R-UNL-2024).

7. 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.

