



Universidad
Nacional
de Loja

Dirección de
Tecnologías de Información

[POLÍTICA]

POLÍTICA DE INFRAESTRUCTURA TECNOLÓGICA

Versión 26.08

Agosto 2026

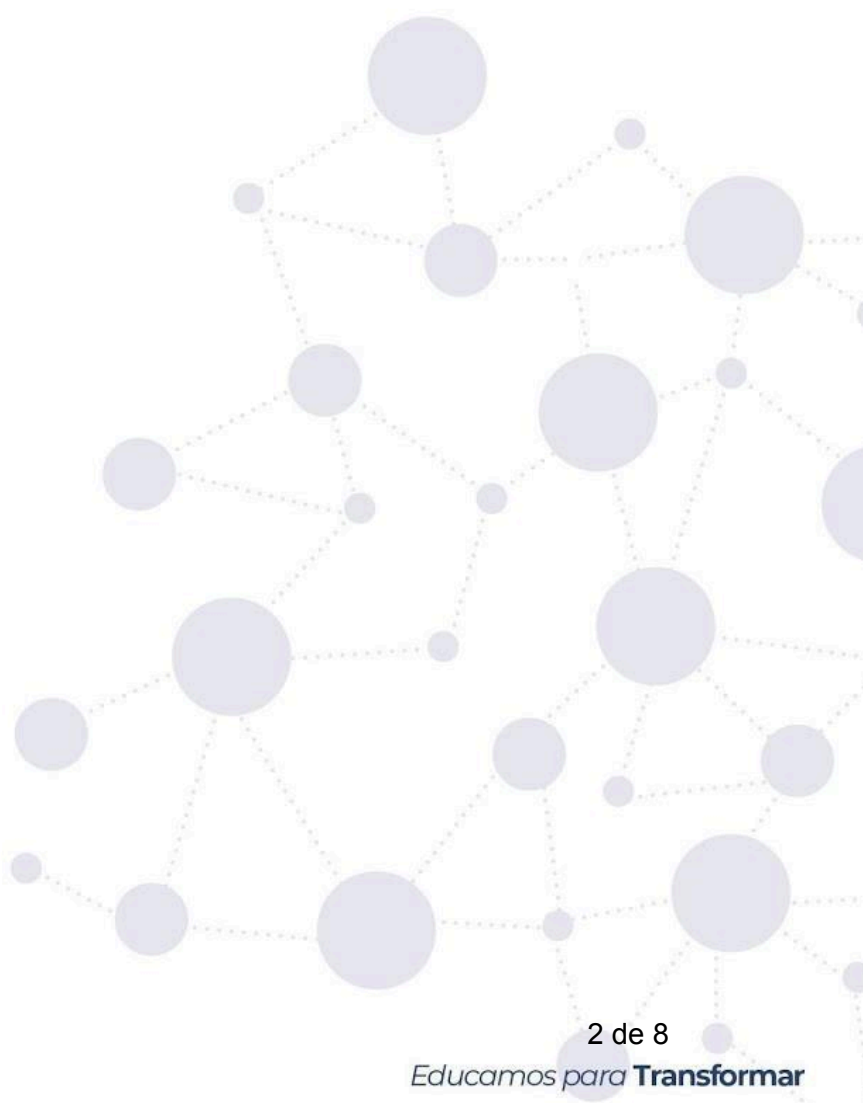
1 de 8

Educamos para **Transformar**



HISTORIAL DE CAMBIOS

Versión	Fecha	Responsable	Descripción de la modificación
26.08	13/08/2027	Ing. Juan Carlos Riofrío Herrera	Documento inicial



CONTENIDOS

1. Objetivo	3
2. Alcance	3
3. Política	4
4. Lineamientos de la política	4
4.1. Seguridad de redes y sistemas de comunicación	4
4.2. Gestión de servidores e infraestructura	4
4.3. Gestión de obsolescencia y ciclo de vida	6
4.4. Equipamiento audiovisual y computadoras	6
4.5. Administración de seguridad perimetral	6
5. Validez y gestión del documento	7
6. Glosario de términos	7
7. Documentos de Referencia	7
8. Firmas de responsabilidad	8

1. Objetivo

Establecer los lineamientos y controles técnicos para la gestión, mantenimiento, protección y renovación de la infraestructura tecnológica (centro de datos, servidores, redes de datos y equipamiento audiovisual) de la Universidad Nacional de Loja (UNL). El propósito es mitigar los riesgos por obsolescencia, proteger la integridad de los sistemas críticos y garantizar la alta disponibilidad de los servicios académicos y administrativos para asegurar la continuidad institucional.

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 tengan acceso físico o privilegios de administración y/o configuración sobre la infraestructura tecnológica propiedad de la UNL. Comprende la infraestructura física, lógica e híbrida de la institución, esto es: el Centro de Datos Institucional (CDI), redes de datos (WAN/LAN/WLAN), servidores (físicos y virtuales) y equipamiento audiovisual (proyectores, pantallas multimedia y/o inteligentes).

3. Política

La Universidad Nacional de Loja a través de la Dirección de Tecnologías de Información (DTI) gestionará su infraestructura tecnológica enfocándose en estrategias de resiliencia, eficiencia y seguridad proactiva. La institución mantendrá su infraestructura tecnológica actualizada, con esquemas de alta disponibilidad, redundancia en componentes críticos, garantía técnica vigente, soporte técnico especializado formal de fabricantes o proveedores autorizados y un ciclo permanente de mitigación de vulnerabilidades técnicas.

4. Lineamientos de la política

4.1. Seguridad de redes y sistemas de comunicación

La DTI debe segmentar la red institucional de forma física y lógica (VLAN), separando el tráfico de administración, servicios críticos, red académica y red para estudiantes y visitantes, para evitar el movimiento lateral de ataque.

La DTI debe mantener diagramas de red y archivos de configuración actualizados y protegidos contra acceso no autorizado.

Los medios de transmisión (fibra óptica y cobre) deben estar debidamente etiquetados, protegidos en canaletas o tuberías adecuadas para evitar daños accidentales, sabotajes o interferencias.

Los puntos de acceso inalámbrico en el campus deben utilizar protocolos de cifrado robustos y autenticación centralizada.

La DTI debe implementar y administrar un sistema de Control de Acceso a la Red (NAC, por sus siglas en inglés) para garantizar que todo dispositivo que intente conectarse a la infraestructura de red institucional, tanto alámbrica como inalámbrica, sea previamente identificado, autenticado y evaluado. Únicamente los dispositivos que cumplan con los perfiles y políticas de seguridad de la UNL (tales como actualizaciones al día y software de protección activo) tendrán autorización para acceder a los recursos de la red interna. Los dispositivos no identificados o que no cumplan con las políticas establecidas deberán ser bloqueados o asignados automáticamente a una red aislada (cuarentena o invitados) con privilegios de acceso estrictamente limitados para evitar el riesgo de comprometer la infraestructura.

4.2. Gestión de servidores e infraestructura

Toda la infraestructura tecnológica debe ser configurada bajo estándares de endurecimiento (hardening), eliminando servicios, protocolos y puertos que no sean estrictamente necesarios para su función.

Se debe implementar una solución de monitoreo que supervise en tiempo real el estado de salud, capacidad y disponibilidad de servidores y equipos de red, enviando alertas automáticas ante fallos.

El acceso a las interfaces de gestión de la infraestructura debe restringirse a redes de administración específicas y, adicionalmente, cumplir con lo establecido en la "Política de Control de Acceso Lógico".

Se prohíbe la instalación de hardware en el Centro de Datos Institucional que carezca de garantía técnica vigente, soporte técnico especializado formal de fabricantes o proveedores autorizados.

Se prohíbe la instalación de equipos de comunicación y red (switches, APs, routers, entre otros) en cualquier área del campus sin la previa autorización, configuración e inventario formal por parte de la DTI. Los dispositivos no autorizados detectados, serán desconectados, retirados y/o bloqueados automáticamente.

La DTI deberá aplicar plantillas de configuración segura (*Hardening*) para cada tipo de activo (servidores, Firewalls, Switches), las cuales serán revisadas periódicamente para asegurar que no existan servicios vulnerables activos.

Los equipos de red y servidores deben mantener su firmware y sistema operativo actualizados a las versiones estables más recientes recomendadas por el fabricante.

La DTI debe llevar a cabo análisis periódicos de vulnerabilidades sobre la infraestructura para identificar y mitigar fallos antes de que sean explotados.

Los cambios y parches deben ejecutarse en horarios que minimicen el impacto académico y administrativo, siguiendo un procedimiento de gestión de cambios.

El Centro de Datos Institucional debe estar conectado a un sistema de energía ininterrumpida (UPS) y, a una línea de energía conectada al menos a un generador eléctrico de respaldo.

El Centro de Datos Institucional y cuartos de telecomunicaciones deben mantener condiciones tecnológicas ambientales óptimas.

Se prohíbe explícitamente el ingreso de comida, bebidas o materiales inflamables al Centro de Datos Institucional y nodos de red.

Los cables de potencia (energía) deben estar físicamente separados de los cables de comunicaciones (datos) para evitar interferencias electromagnéticas.

Es obligatorio mantener las puertas del Centro de Datos Institucional cerradas y bloqueadas en todo momento, evitando que queden abiertas sin supervisión.

4.3. Gestión de obsolescencia y ciclo de vida

La DTI mantendrá un inventario actualizado de las fechas de adquisición, fecha y periodo de vigencia de garantía de cada equipo crítico.

Se deben establecer estrategias de renovación tecnológica anual para sustituir equipos que alcancen el término de su vida útil, priorizando aquellos que ya no reciben actualizaciones de seguridad.

Antes de dar de baja o transferir equipos del CDI se debe realizar un borrado seguro de toda la información residual.

4.4. Equipamiento audiovisual y computadoras

Los proyectores, pantallas interactivas y sistemas de videoconferencia deben estar integrados en el plan de mantenimiento preventivo de la DTI. Asimismo, es responsabilidad del personal docente y administrativo que usan o están a cargo de los espacios físicos institucionales, velar por la custodia y aplicación constante de las medidas de seguridad física (control de accesos, aseguramiento de puertas y resguardo de periféricos) para evitar la sustracción, pérdida o manipulación no autorizada de estos equipos.

Las computadoras institucionales en laboratorios y oficinas deben ser estandarizadas en hardware y configuración para facilitar su soporte y actualización masiva.

Todo hardware que requiera software propietario para su funcionamiento (ej. controladores, sistemas operativos de red) debe contar con las licencias vigentes.

4.5. Administración de seguridad perimetral

La DTI administrará los dispositivos de borde (firewalls) bajo el principio de "denegación por defecto".

Se mantendrá un registro de reglas de acceso, el cual será objeto de una revisión técnica periódica por parte de la DTI a fin de depurar reglas obsoletas o inseguras.

El acceso a la infraestructura desde redes externas (Internet) se realizará exclusivamente mediante canales cifrados (VPN).

5. 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.

6. Glosario de términos

Término	Definición
Endurecimiento (Hardening)	Proceso de asegurar un sistema (servidor o equipo de red) mediante la reducción de vulnerabilidades a través de la eliminación de funciones y protocolos innecesarios.
Firmware	Programa básico e inalterable que controla el funcionamiento de los circuitos electrónicos de un dispositivo de hardware (ej. switches, routers).
Gestión de Parches	Proceso sistemático de identificar, probar e instalar actualizaciones de software o seguridad para corregir errores o vulnerabilidades detectadas.
Mantenimiento Preventivo	Acciones planificadas realizadas sobre el hardware para reducir la probabilidad de fallo o degradación de los servicios.
Obsolescencia Tecnológica	Condición en la que un equipo deja de ser seguro o eficiente debido a que el fabricante ha finalizado su soporte técnico o ya no existen repuestos ni actualizaciones.
SLA (Service Level Agreement)	Acuerdo de Nivel de Servicio; compromiso formal (con proveedores) que define los tiempos de respuesta y disponibilidad garantizados para un equipo.
UPS (Uninterruptible Power Supply)	Sistema de energía ininterrumpida que proporciona energía eléctrica mediante baterías de forma inmediata ante un corte de luz, protegiendo equipos sensibles.

7. 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 2.11, 3.12, 3.13, 4.8, 4.9
- 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).

8. 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.