



Universidad
Nacional
de Loja

Dirección de
Tecnologías de Información

[POLÍTICA]

POLÍTICA DE USUARIOS FINALES

Versión 26.08

Agosto 2026



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. Uso aceptable de los recursos y sistemas de información	4
4.2. Gestión de credenciales, autenticación y control de acceso	5
4.3. Uso de dispositivos personales (BYOD) dentro del campus y trabajo remoto	6
4.4. Protección de datos personales e información confidencial	6
4.5. Uso del correo electrónico institucional y herramientas colaborativas	6
4.6. Prohibiciones explícitas	7
4.7. Interacción con proveedores tecnológicos externos	8
4.8. Custodia de equipos portátiles	8
4.9. Supervisión y monitoreo de los recursos tecnológicos	8
4.10. Reporte de incidentes de seguridad y solicitud de requerimientos	9
4.11. Validez y gestión del documento	9
5. Glosario de términos	9
6. Documentos de Referencia	10
7. Firmas de responsabilidad	11

1. Objetivo

Establecer las directrices formales para el uso aceptable, seguro y responsable de los sistemas de información, infraestructura tecnológica, servicios digitales y dispositivos personales dentro de la Universidad Nacional de Loja (UNL). Este documento busca garantizar la confidencialidad, integridad y disponibilidad de la información institucional, salvaguardando los datos personales de la comunidad universitaria alineando el comportamiento de los usuarios finales con el Esquema Gubernamental de Seguridad de la Información, la normativa legal ecuatoriana y las mejores prácticas internacionales.

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, generen, procesen o custodien información de la UNL. En adelante en este documento, el uso del término "usuario final" o "usuarios finales" engloba a todos los grupos mencionados anteriormente. Aplica al uso de la infraestructura tecnológica institucional (redes, servidores), sistemas académicos, plataformas virtuales de aprendizaje, sistemas administrativos y financieros, así como al uso de dispositivos personales (BYOD) dentro del campus universitario o mediante conexiones de trabajo remoto.

3. Política

Controlar y proteger el uso de los sistemas y recursos tecnológicos de la UNL por parte de todos los usuarios finales, asegurando que el acceso y procesamiento de la información, incluidos los datos personales y académicos, se realice bajo estrictos parámetros de seguridad, cumplimiento normativo y ética profesional, mitigando riesgos cibernéticos e incidentes de seguridad.

4. Lineamientos de la política

4.1. Uso aceptable de los recursos y sistemas de información

Los recursos tecnológicos provistos por la UNL, son para uso exclusivo de las actividades institucionales, administrativas, académicas, de investigación y vinculación con la sociedad. La UNL se reserva el derecho de ejecutar actividades de monitorización detectiva, preventiva y/o reactiva frente a amenazas de seguridad que pudiesen poner en riesgo las operaciones e información.

Es responsabilidad de los usuarios finales usar de forma aceptable y segura los recursos tecnológicos asignados para el desarrollo de sus funciones, tales como equipamiento tecnológico, servicios informáticos y credenciales de acceso.

En caso de identificar en los equipos institucionales que la protección contra malware (virus) no se encuentra instalada, está inactiva o desactualizada, el usuario final deberá reportarlo para su configuración y activación.

La institución ejecutará un monitoreo activo del tráfico de red para prevenir riesgos cibernéticos. Si un usuario final requiere acceso a sitios web restringidos por los filtros de seguridad institucionales, deberá canalizar la solicitud debidamente justificada a través del Sistema de Servicios de TI + Asistente IA (serviciosti.unl.edu.ec).

El comportamiento inusual de usuarios en los servicios e infraestructura tecnológica institucional facultará a la DTI a realizar análisis minuciosos en los equipos y escalar los hallazgos a las instancias correspondientes.

4.2. Gestión de credenciales, autenticación y control de acceso

Las cuentas de usuario y contraseñas son estrictamente personales, confidenciales e intransferibles. Toda actividad realizada con las credenciales institucionales será de entera responsabilidad del usuario final titular de las mismas, asumiendo éste las consecuencias normativas o disciplinarias derivadas de cualquier mal uso o divulgación de dicha información.

Para garantizar una gestión segura, los usuarios finales deben observar rigurosamente las siguientes directrices:

- ➔ Los usuarios deben bloquear la sesión de sus equipos al ausentarse de su puesto de trabajo físico o remoto, mediante la configuración automática de bloqueo de pantalla protegido por pin de acceso o contraseña. Se establecerá el bloqueo automático de pantalla con un tiempo no superior a 5 minutos.
- ➔ Es obligatorio mantener una práctica de escritorio limpio; esto implica que al finalizar la jornada o al ausentarse del área de trabajo, no deben dejarse a la vista documentos impresos, libretas, notas adhesivas (post-its) con contraseñas, medios de almacenamiento o cualquier otro soporte físico que contenga información institucional relevante o confidencial, mitigando así el riesgo de accesos físicos no autorizados.
- ➔ Los usuarios finales tendrán acceso exclusivo a los sistemas y plataformas de la UNL para los cuales cuenten con autorización formal, en estricto cumplimiento de sus funciones académicas, operativas o administrativas. Queda terminantemente prohibido ejecutar acciones que busquen eludir los controles de seguridad perimetral o de aplicaciones, tales como: uso o suplantación de credenciales pertenecientes a otro usuario final, ejecución de procesos, scripts o acciones no autorizadas dentro de la red institucional e implementación o uso de redes privadas virtuales (VPN) personales para evadir el filtrado de tráfico.

4.3. Uso de dispositivos personales (BYOD) dentro del campus y trabajo remoto

Cuando los usuarios finales utilicen sus equipos personales (ordenadores portátiles, tabletas, teléfonos inteligentes u otros dispositivos) para el desarrollo de actividades académicas o administrativas, deberán cumplir con los siguientes lineamientos:

- La conexión de dispositivos personales a la red institucional de la UNL estará sujeta a validación y a la aplicación de los controles de seguridad que la institución determine oportunos.
- Todo equipo personal utilizado para acceder a sistemas de información institucionales o plataformas virtuales que procesan datos de la UNL debe contar con protección de antivirus actualizada.
- En la modalidad de trabajo remoto, el acceso a los sistemas administrativos y financieros deberá realizarse mediante conexiones seguras y autorizadas, cumpliendo con la “Política de Teletrabajo” a fin de proteger la información procesada fuera de las instalaciones de la UNL.

4.4. Protección de datos personales e información confidencial

En estricto cumplimiento de la Ley Orgánica de Protección de Datos Personales, todo usuario final que procese datos personales de responsabilidad de la UNL debe garantizar la confidencialidad y el sigilo.

Queda prohibida la extracción, descarga masiva o transferencia no autorizada de bases de datos desde los sistemas académicos y financieros hacia medios de almacenamiento externo (USB, discos duros) o repositorios en la nube no institucionales.

El tratamiento de datos personales, especialmente aquellos considerados sensibles (salud, etnia, etc.), requiere de medidas de seguridad reforzadas y no deben ser compartidos a través de canales de comunicación no seguros.

4.5. Uso del correo electrónico institucional y herramientas colaborativas

El correo electrónico bajo el dominio institucional y las herramientas de productividad y colaboración en la nube deben emplearse exclusivamente para fines inherentes a las funciones universitarias.

Queda prohibido utilizar la cuenta de correo institucional para registrarse o suscribirse en plataformas, servicios o sitios web ajenos a las actividades académicas, de investigación o administrativas de la institución.

Las cuentas de correo operadas bajo el dominio de la UNL son herramientas oficiales; por ende, toda información cursada o almacenada en ellas posee el carácter de información institucional. La UNL se reserva el derecho de auditar proactivamente este servicio para mitigar amenazas y asegurar la continuidad operativa.

Los usuarios finales deben abstenerse de interactuar con correos no solicitados, evitar el reenvío de cadenas, y reportar inmediatamente cualquier mensaje anómalo o intento de suplantación de identidad (phishing). La difusión de comunicados masivos será potestad exclusiva de las áreas expresamente autorizadas.

4.6. Prohibiciones explícitas

Con el fin de preservar la confidencialidad, integridad y disponibilidad de la infraestructura y los datos de la institución, queda estrictamente prohibido para los usuarios finales:

- ➔ Manipular, desinstalar, inhabilitar o intentar eludir los mecanismos de protección implementados por la institución en su infraestructura y equipos de trabajo, incluyendo software antivirus, firewalls, controles perimetrales o políticas de red.
- ➔ Utilizar la red institucional y los servicios de internet para la descarga, almacenamiento o divulgación de software, documentos, material audiovisual o cualquier otro contenido que vulnere los derechos de autor, licenciamientos, marcas o patentes comerciales.
- ➔ Instalar programas, aplicaciones o conectar dispositivos externos (como módems, tarjetas de red, unidades de almacenamiento u otros periféricos) en los equipos de dotación sin la aprobación previa de la DTI. Toda instalación permitida deberá ser ejecutada previa autorización de la DTI, gestionando esta actividad mediante un ticket de soporte oficial.
- ➔ Realizar escaneos de puertos, intercepción de tráfico o pruebas de vulnerabilidad en la infraestructura tecnológica sin autorización formal.
- ➔ Aplicar herramientas o métodos de cifrado de disco o de carpetas de forma personal y no centralizada en los equipos institucionales, lo cual impide la recuperación de activos de información por parte de la UNL.
- ➔ Descargar, almacenar o emplear códigos maliciosos, generadores de claves, herramientas de explotación (hacking), así como el uso de proxys o servicios anonimizadores diseñados para ocultar el tráfico y evadir el filtrado de navegación web de la universidad.
- ➔ Acceder a sistemas, dispositivos, recursos informáticos o credenciales que no le hayan sido designados formalmente.
- ➔ Extraer, exponer o revelar de manera ilícita el contenido de bases de datos, registros, expedientes o archivos institucionales, comprometiendo el sigilo,

la intimidad y la protección de datos personales de cualquier miembro de la comunidad universitaria.

- Emplear los recursos tecnológicos para alojar, visualizar, descargar o distribuir material que sea sexualmente explícito, difamatorio, violento, perturbador; fomente cualquier tipo de actividad ilegal; o promueva la discriminación por motivos de nacionalidad, etnia, sexo, orientación sexual, estado civil, edad, discapacidad, afinidad religiosa, política u otras.
- Destinar la infraestructura, los activos de información o los servicios de la UNL para fines estrictamente personales, actividades comerciales ajenas a las funciones universitarias, o cualquier acción que exponga la postura de seguridad de la institución.

4.7. Interacción con proveedores tecnológicos externos

Los usuarios finales que deban coordinar actividades con proveedores externos asegurarán que dichos terceros no accedan a los sistemas o datos institucionales sin la previa suscripción de acuerdos de confidencialidad y la asignación formal de credenciales con privilegios limitados al servicio prestado, además deberá cumplir con los lineamientos descritos en la “Política de Relación con Proveedores”.

4.8. Custodia de equipos portátiles

Los usuarios finales que movilicen equipos tecnológicos institucionales (laptops, tabletas, medios de almacenamiento) fuera de los entornos protegidos de la UNL, asumen la responsabilidad de extremar precauciones para mitigar los riesgos de hurto, extravío o acceso ilegítimo.

Es obligatorio mantener las soluciones de protección contra software malicioso. En espacios públicos o de libre concurrencia, el usuario debe resguardar la pantalla de visualizaciones no autorizadas y mantener la custodia física permanente del equipo, evitando dejarlo sin supervisión en entornos no controlados.

4.9. Supervisión y monitoreo de los recursos tecnológicos

Dentro del enfoque holístico que enmarca la seguridad de la información, todo dato generado, transmitido o almacenado en la infraestructura de la UNL (incluyendo la navegación web y el correo electrónico) es considerado propiedad institucional.

Al utilizar estos recursos, los usuarios finales reconocen y aceptan que la universidad, a través del personal autorizado, tiene la potestad de implementar herramientas especializadas para monitorear el flujo de información, bloquear tráfico malicioso, filtrar contenidos prohibidos y auditar registros de actividad.

Estas medidas preventivas buscan salvaguardar los activos de la institución y no se considerarán una vulneración a la privacidad personal en el ámbito del ejercicio de sus funciones.

4.10. Reporte de incidentes de seguridad y solicitud de requerimientos

El medio oficial para realizar cualquier tipo de requerimiento o reporte de incidentes será el Sistema de Servicios de TI + Asistente IA (serviciosti.unl.edu.ec) provisto por la universidad.

Todo usuario final que sospeche o tenga conocimiento de un incidente de seguridad (pérdida de equipos, exposición de contraseñas, infección por virus, acceso no autorizado a sistemas académicos o financieros, entre otros.) tiene la obligación de reportarlo inmediatamente.

4.11. 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
Usuarios finales	Toda persona (estudiantes, docentes, personal administrativo, trabajadores, alumni y terceros autorizados) que tiene acceso, interactúa o procesa datos a través de la infraestructura tecnológica, sistemas de información y recursos digitales de la Universidad Nacional de Loja.
Holístico	Perspectiva de gestión e implementación que aborda la seguridad de la información de manera integral, interconectando aspectos tecnológicos, normativos, organizacionales, procesos y el factor humano, en lugar de tratarlos como componentes aislados.
Dispositivos personales (BYOD/ Bring Your Own Device)	Equipos tecnológicos de propiedad del usuario final (teléfonos inteligentes, tabletas, computadoras portátiles) que son utilizados para acceder, procesar o almacenar información y recursos de la red institucional, requiriendo controles específicos para mitigar riesgos sobre los activos de información.
Acceso Remoto	Es la capacidad de conectarse a las computadoras, servidores o sistemas internos de la universidad desde otro lugar (fuera del

	campus de la UNL) a través de internet, utilizando herramientas seguras para trabajar o estudiar a distancia.
Inicio de sesión único (SSO)	Mecanismo de control de acceso y autenticación centralizada que permite a los usuarios finales acceder a múltiples aplicaciones, sistemas y plataformas institucionales de manera segura, utilizando un único conjunto de credenciales.
Doble Factor de Autenticación (2FA)	Medida de seguridad adicional para el control de acceso que exige al usuario confirmar su identidad mediante dos métodos de validación independientes (usualmente algo que el usuario "sabe", como una contraseña, y algo que "posee", como un código generado en una aplicación móvil), dificultando la suplantación de identidad.
Escritorio Limpio	Práctica organizativa de seguridad física que obliga a los usuarios finales a mantener sus áreas de trabajo despejadas de soportes físicos que contengan información sensible o confidencial (documentos impresos, medios de almacenamiento extraíbles, notas con contraseñas) al finalizar la jornada o al ausentarse del puesto, previniendo accesos visuales o físicos no autorizados.
Sigilo	Obligación legal, técnica y ética de mantener estricta reserva, secreto y máxima confidencialidad respecto a la información institucional y los datos personales (especialmente los sensibles) a los que un usuario tiene acceso en el ejercicio de sus funciones, garantizando su no divulgación a terceros no autorizados.
Bases de datos	Conjunto organizado, estructurado y centralizado de información (que puede incluir datos personales, académicos, financieros o administrativos) almacenado sistemáticamente en un medio físico o electrónico para su tratamiento, consulta y gestión, constituyendo un activo de información crítico que requiere medidas técnicas y organizativas de protección.
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.

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 y su Reglamento.

- 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 1.10, 1.11, 1.14, 1.17, 1.32, 2.7, 3.7, 3.9, 3.10, 4.1, 4.7, 4.13, 4.19
- 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.

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.