



Universidad
Nacional
de Loja

Dirección de
Tecnologías de Información

[POLÍTICA]

POLÍTICA DE TELETRABAJO

Versión 26.08

Agosto 2026

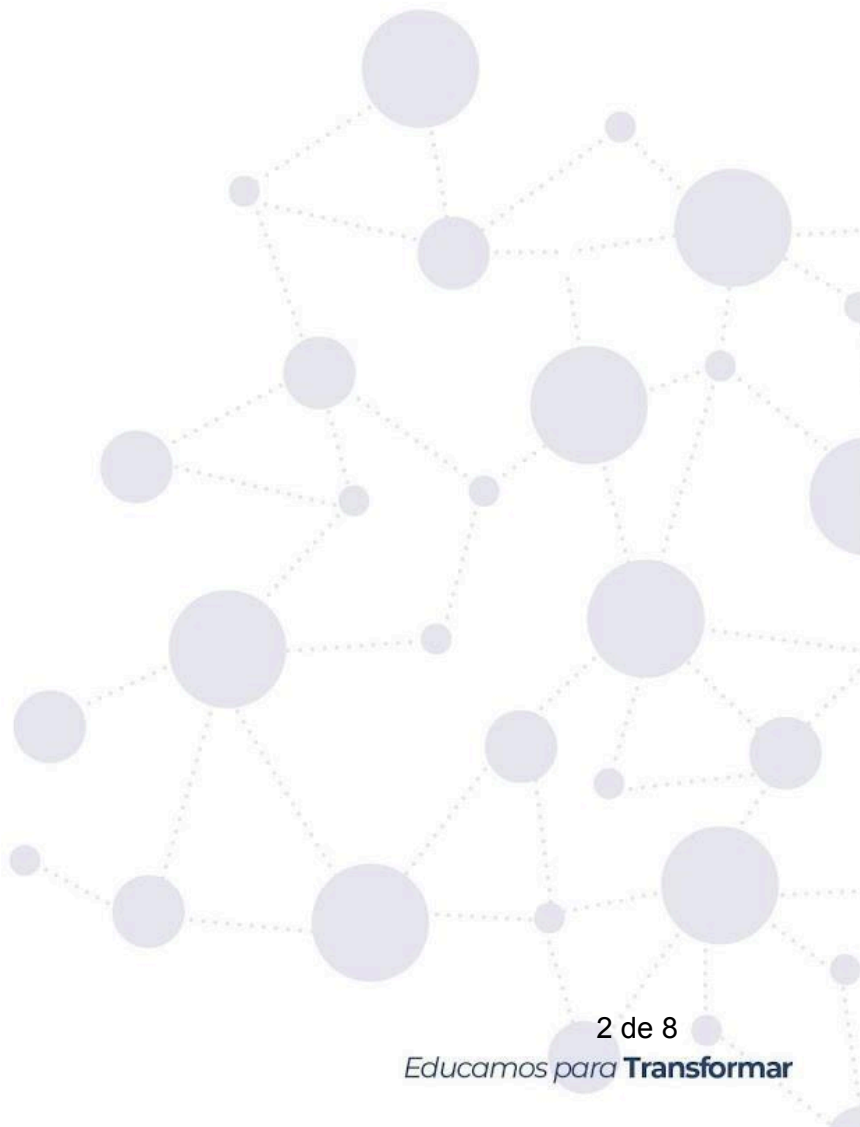
1 de 8

Educamos para **Transformar**



HISTORIAL DE CAMBIOS

Versión	Fecha	Responsable	Descripción de la modificación
26.08	13/08/2026	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. Disposición de activación de la modalidad de teletrabajo	4
4.2. Controles de acceso e identidad	4
4.3. Confidencialidad y buen uso de la información	5
4.4. Validez y gestión del documento	5
5. Glosario de términos	6
6. Documentos de Referencia	7
7. Firmas de responsabilidad	8

1. Objetivo

Establecer los lineamientos, controles y responsabilidades para proteger la confidencialidad, integridad y disponibilidad de la información institucional durante la ejecución de actividades laborales fuera de las instalaciones de la Universidad Nacional de Loja (UNL), para garantizar el resguardo de los activos frente a amenazas en entornos no controlados.

2. Alcance

Esta política es de cumplimiento obligatorio para la comunidad universitaria y terceros, conforme al alcance y usuarios definidos en la Política de Seguridad de la Información, que accedan a la infraestructura tecnológica institucional (redes, servidores, servicios TI) desde ubicaciones externas, aplicándose tanto al uso de equipos provistos por la institución como a dispositivos personales (BYOD).

3. Política

La Universidad Nacional de Loja garantiza la seguridad de la información en entornos de trabajo remoto, estableciendo el marco de actuación para que el personal de la UNL ejecute sus labores fuera del campus, garantizando que el acceso a la infraestructura tecnológica y el tratamiento de los datos se realicen bajo los mismos estándares de seguridad exigidos dentro de la institución.

4. Lineamientos de la política

4.1. Disposición de activación de la modalidad de teletrabajo

La modalidad de trabajo remoto o teletrabajo será aprobada por la máxima autoridad de la UNL o su delegado/a, previa solicitud sustentada y estudio técnico elaborado por la Dirección de Talento Humano.

4.2. Controles de acceso e identidad

Todo acceso a los sistemas informáticos y servicios tecnológicos de la institución, desde ubicaciones remotas deberá realizarse mediante canales cifrados utilizando redes privadas virtuales (VPN) autorizadas por la DTI. El personal en modalidad remota debe dar cumplimiento estricto a la "Política de Usuarios Finales".

Se prohíbe el uso de redes Wi-Fi públicas o no cifradas para el acceso a sistemas institucionales.

4.3. Confidencialidad y buen uso de la información

El personal que acceda a información institucional desde ubicaciones remotas debe observar el principio de confidencialidad, asegurando que los datos no sean tratados o comunicados para un fin distinto para el cual fueron recogidos.

Queda estrictamente prohibida la descarga, almacenamiento local o replicación de bases de datos que contengan datos personales o sensibles en dispositivos personales o medios de almacenamiento extraíbles no cifrados.

En los entornos de trabajo remoto, se debe considerar la amenaza de acceso no autorizado a información o recursos por parte de otras personas presentes en el lugar (por ejemplo, familiares y amigos), por lo que se deberá restringir el acceso a dispositivos personales a terceros.

Para garantizar el no repudio, la integridad y la autoría de los actos administrativos y académicos generados fuera del campus, el personal deberá suscribir los documentos oficiales utilizando firma electrónica mediante los sistemas informáticos autorizados.

Toda operación institucional en modalidad remota deberá estar respaldada con evidencia digital suficiente y pertinente que sustente su veracidad, permitiendo su seguimiento y comprobación.

El personal está en la obligación de informar los eventos de seguridad de la información (tales como la pérdida de un dispositivo, sospecha de infección por malware o accesos no autorizados) para prevenir o minimizar el efecto de los incidentes de seguridad.

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
Trabajo remoto o teletrabajo	Modalidad laboral en la cual el personal de la institución ejecuta sus actividades, responsabilidades académicas o administrativas fuera de las instalaciones físicas de la universidad (por ejemplo, desde su domicilio). Para ello, utiliza tecnologías de la información y comunicación (TIC) que le permiten acceder a los sistemas, plataformas y datos institucionales a distancia.
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.
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.
Redes Wi-Fi públicas	Redes inalámbricas de acceso a Internet disponibles en lugares abiertos al público (como cafeterías, parques, aeropuertos o centros comerciales) que generalmente carecen de medidas de seguridad sólidas o cifrado de datos. Representan un alto riesgo de vulnerabilidad, ya que los ciberdelincuentes pueden interceptar fácilmente el tráfico; por ello, su uso para acceder a sistemas institucionales críticos está restringido y requiere obligatoriamente el uso de una VPN.
FirmaEC	Plataforma informática oficial desarrollada por el Estado ecuatoriano que permite la validación y firma de documentos electrónicos. En el entorno institucional, se utiliza en conjunto con un certificado de firma electrónica válido para suscribir documentos, garantizando la autenticidad (quién es el autor), la integridad (que el documento no ha sido alterado) y el no repudio (la imposibilidad de negar la autoría) de los actos administrativos y académicos.
Incidentes de seguridad	Cualquier evento anómalo o adverso, ya sea confirmado o bajo sospecha, que amenaza o compromete la confidencialidad, integridad o disponibilidad de la información institucional o los

Término	Definición
	sistemas tecnológicos. Ejemplos de estos incidentes incluyen: el robo o extravío de un dispositivo móvil, infecciones por software malicioso (malware/ransomware), intentos de <i>phishing</i> (suplantación de identidad), vulneración de bases de datos o accesos no autorizados a las cuentas de usuario de la universidad, entre otros.

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 2.7.
- 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.