



Universidad  
Nacional  
de Loja

Dirección de  
Tecnologías de Información

[POLÍTICA]

# POLÍTICA DE CONTROL DE ACCESO

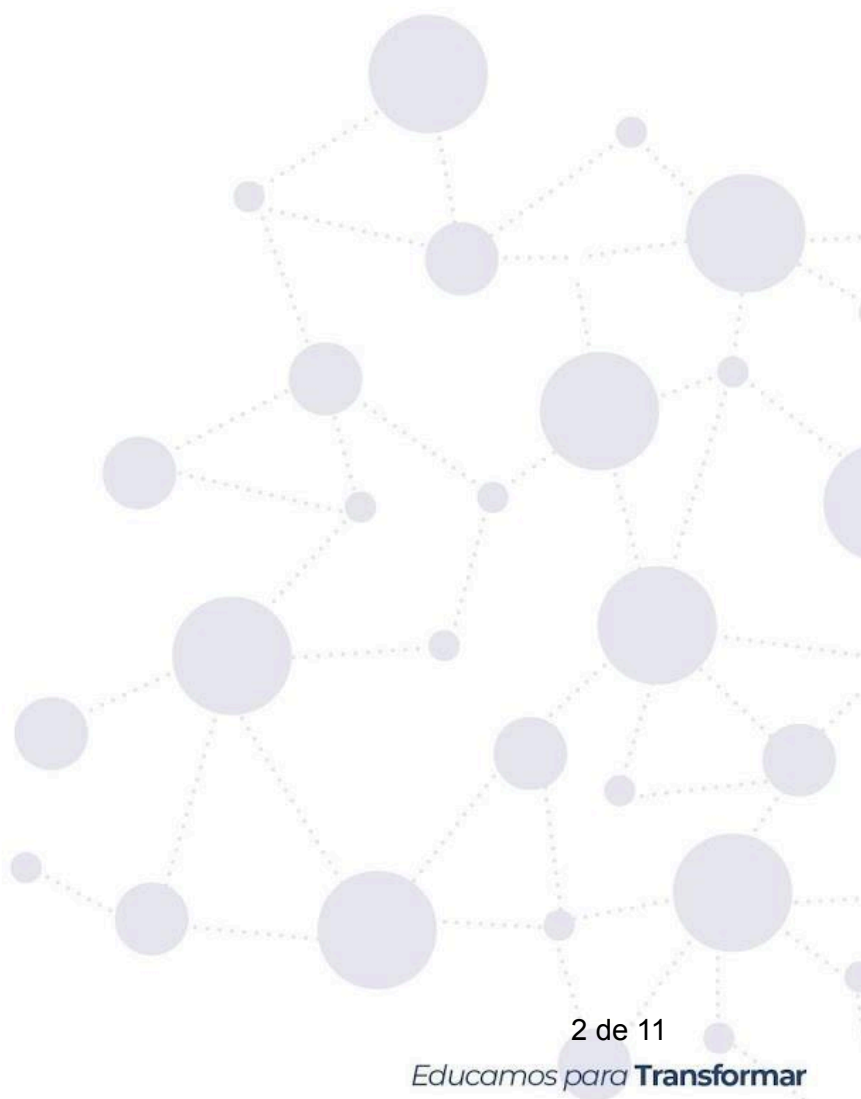
Versión 26.08

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

|                                                         |           |
|---------------------------------------------------------|-----------|
| <b>1. Objetivo</b>                                      | <b>4</b>  |
| <b>2. Alcance</b>                                       | <b>4</b>  |
| <b>3. Política</b>                                      | <b>4</b>  |
| <b>4. Lineamientos de la política</b>                   | <b>4</b>  |
| 4.1. Gestión de identidades y ciclo de vida del usuario | 4         |
| 4.2. Autenticación y gestión de contraseñas             | 6         |
| 4.3. Cuentas de superusuario                            | 7         |
| 4.4. Auditoría de cuentas                               | 8         |
| 4.5. Acceso físico                                      | 8         |
| 4.6. Validez y gestión del documento                    | 8         |
| <b>5. Glosario de términos</b>                          | <b>9</b>  |
| <b>6. Documentos de referencia</b>                      | <b>10</b> |
| <b>7. Firmas de responsabilidad</b>                     | <b>11</b> |

## 1. Objetivo

Establecer los lineamientos, controles y responsabilidades para garantizar que el acceso a los activos, sistemas de información e infraestructura tecnológica de la Universidad Nacional de Loja sea concedido únicamente a usuarios autorizados, bajo los principios de "necesidad de saber" y "mínimo privilegio", mitigando riesgos de acceso no autorizado o fuga de datos.

## 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 requieran acceso a la red o sistemas institucionales. Su aplicación abarca la totalidad de los activos de información (sistemas de información, bases de datos, servidores, infraestructura tecnológica), y se extiende a los dispositivos personales (BYOD) que interactúen con la infraestructura tecnológica de la UNL.

## 3. Política

La Universidad Nacional de Loja garantiza que todos los accesos a sus recursos lógicos y físicos sean gestionados de forma centralizada, segura y auditable, para lo cual se provee de los lineamientos a seguir para garantizar la confidencialidad, integridad y disponibilidad de la información mediante un adecuado control de acceso.

## 4. Lineamientos de la política

### 4.1. Gestión de identidades y ciclo de vida del usuario

La creación, modificación, asignación de roles y desactivación de cuentas institucionales operará de forma centralizada utilizando el módulo de Seguridad Informática (MSI) en el SIAAF, asegurando la trazabilidad de cada perfil y evitando la proliferación de cuentas huérfanas.

El registro de nuevos usuarios institucionales (estudiantes o funcionarios) debe estar vinculado a un proceso formal de matrícula o contratación.

La Dirección de Tecnologías de Información debe mantener un inventario de usuarios y los accesos que mantiene, así como un histórico de cada uno de estos.

El acceso a los recursos tecnológicos institucionales exige el uso de credenciales únicas, personales e intransferibles. Queda prohibido el préstamo o compartición de credenciales de acceso. Los cambios de roles o nuevos roles asignados serán gestionados y actualizados inmediatamente en el SIAAF.

En cumplimiento con los principios de control interno y gestión de riesgos, la UNL aplicará una estricta segregación de funciones para mitigar el riesgo de uso indebido, fraude o modificación no autorizada en los activos de información. Ningún usuario o administrador concentrará los privilegios necesarios para solicitar, autorizar y aprovisionar un acceso de forma unilateral; todo flujo de asignación de roles deberá involucrar distintos responsables dentro del SIAAF.

La validación y autorización para la creación/habilitación de usuarios para docentes, administrativos y trabajadores se realizará desde la Dirección de Talento Humano y la validación y autorización para la creación/habilitación de usuarios para estudiantes se realizará desde las diferentes direcciones, según el siguiente detalle:

| Estamento                       | Responsable                              |
|---------------------------------|------------------------------------------|
| Carreras de grado               | Vicerrectorado Académico                 |
| Programas de posgrado           | Dirección de posgrados                   |
| Programas de educación continua | Dirección de Vinculación con la Sociedad |

En los casos que corresponda, la DTI facilitará las herramientas informáticas necesarias para esta gestión.

La gestión de usuarios para las personas externas o terceros será tramitada mediante solicitud formal.

Para funcionarios que soliciten accesos a los sistemas institucionales y que no tienen relación con su contrato, ya sea por un encargo, subrogación, o como responsable de un proyecto, deberá legalizar una solicitud de acceso que contará con la firma de responsabilidad del funcionario solicitante y la firma de autorización expresa de su jefe inmediato superior. Como excepción a este flujo normativo, y con el objetivo de optimizar la eficiencia administrativa, cuando el solicitante sea un Director Departamental o un funcionario cuyo jefe inmediato superior sea el Rector/a o Vicerrector/a, bastará únicamente con la firma del solicitante y el documento habilitante.

Cualquier usuario que solicite o tenga acceso a un sistema de información deberá aceptar y cumplir obligatoriamente el acuerdo de confidencialidad y buen uso de sistemas institucionales.

En el caso de funcionarios, será requisito indispensable que la Dirección de Talento Humano(DTH) realice la asignación de puestos en el SIAAF, para en lo posterior otorgar las credenciales y roles correspondientes.

La terminación de la relación contractual, cese de funciones o pérdida de la condición de funcionario de la UNL, conlleva la revocación de todos los privilegios y accesos lógicos a los sistemas institucionales. Ante situaciones excepcionales debidamente justificadas, la dependencia competente podrá autorizar la habilitación temporal de credenciales (se debe detallar fecha de inicio y fin de los accesos), debiendo registrar dicha excepción en el módulo de seguridad del SIAAF para garantizar la trazabilidad de la gestión.

Para el estamento estudiantil, la pérdida de la condición de usuario activo y la consecuente modificación de privilegios se determinará por la obtención del grado académico (transición al estamento de alumni) o por la interrupción del programa de estudios por un periodo de hasta diez (10) años, de acuerdo con el *"Reglamento de Régimen Académico de la Universidad Nacional de Loja"*.

Como medida de apoyo a la gestión administrativa posgraduación, las credenciales de acceso mediante el sistema de Autenticación Única (SSO) y 2FA permanecerán vigentes por un periodo de un (1) año calendario posterior a la fecha de registro del título, tras lo cual se procederá a la baja o reasignación de perfiles según se requiera.

Se desalienta el uso de cuentas genéricas, salvo aquellas destinadas a departamentos, ejecución de procesos automáticos o cuentas de servicio que cuenten con un responsable o custodio debidamente documentado.

#### **4.2. Autenticación y gestión de contraseñas**

Una cuenta de usuario podría tener asociados diferentes perfiles de acceso acorde al rol definido para el personal. Cada perfil establecerá los privilegios del usuario sobre la información alojada en los sistemas.

Para robustecer la protección de cuentas frente a los riesgos de ciberseguridad, es de uso obligatorio el Sistema de Autenticación Única (SSO) integrado de manera mandataria con un Doble Factor de Autenticación (2FA).

Las contraseñas para los distintos perfiles de la UNL deben tener una longitud mínima de 12 caracteres e incluir una combinación algorítmica de letras mayúsculas, minúsculas, números y caracteres especiales no alfanuméricos.

Se establecerá un límite máximo de intentos fallidos de autenticación ( 5 intentos), posterior al cual la cuenta se bloqueará temporalmente para evitar ataques de fuerza bruta.

Se debe renovar la contraseña obligatoriamente al menos una vez cada año, así como en el primer inicio de sesión tras su creación o restablecimiento.

Se debe controlar y restringir el uso en contraseñas de palabras de diccionario, datos personales predecibles (fechas de nacimiento, nombres de familiares) o fragmentos que contengan el propio nombre de usuario.

Como medida proactiva de seguridad y protección de la identidad digital, el sistema generará una notificación automatizada e inmediata ante cualquier evento de cambio de contraseña, restablecimiento de credenciales o modificación en la configuración del Doble Factor de Autenticación (2FA). Esta alerta será enviada de forma simultánea tanto al correo electrónico institucional como al correo electrónico personal registrado por el usuario en el SIAAF. El objetivo de esta doble notificación es permitir que el titular de la cuenta detecte oportunamente cualquier intento de acceso no autorizado o suplantación de identidad, garantizando que el usuario mantenga el control absoluto sobre sus mecanismos de autenticación en todo momento.

Ante cualquier sospecha, evidencia de compromiso o notificación de filtración de credenciales en plataformas externas (Data Breaches), la Dirección de Tecnologías de la Información activará de inmediato el protocolo de contención de identidades. Este procedimiento comprende:

- ➔ La notificación formal del incidente al usuario afectado.
- ➔ La invalidación y restablecimiento forzoso de la contraseña (obligando a su actualización en el próximo inicio de sesión).
- ➔ La activación mandatoria del Doble Factor de Autenticación (2FA) para asegurar la cuenta.

### **4.3. Cuentas de superusuario**

Los permisos de superusuario no se otorgarán por defecto a todo el personal de TI. Solo se asignan a los funcionarios que justifiquen una necesidad técnica real para el cumplimiento de sus funciones diarias, y dichos permisos estarán limitados únicamente a los servidores o sistemas que administran.

Las contraseñas originales de las cuentas de superusuario (las cuentas root nativas) deberán estar protegidas, cifradas y custodiadas de manera segura por la Dirección de Tecnologías de la Información. Su uso directo se limitará exclusivamente a escenarios de emergencia informática (caída total del sistema, desastres o pérdida de acceso delegado).

Todo acceso administrativo remoto a los servidores de la institución debe realizarse obligatoriamente a través de protocolos de comunicación cifrados, estableciendo SSH (Secure Shell) como el estándar único. Para elevar el nivel de seguridad, la autenticación no se basará en contraseñas convencionales, sino en el uso de Infraestructura de Clave Pública (PKI) mediante el intercambio de llaves (pública y privada). Bajo este esquema, el acceso estará permitido únicamente a

los técnicos que posean la llave privada autorizada y debidamente resguardada, quedando estrictamente prohibida la autenticación por contraseña para servicios de administración remota de servidores.

#### **4.4. Auditoría de cuentas**

La gestión de identidades y accesos en la UNL se administra a través del módulo de seguridad informática del SIAAF. Para garantizar la visibilidad, trazabilidad y control de accesos, se establecen los siguientes criterios:

- Las plataformas institucionales se integrarán con el SIAAF para la gestión y control de usuarios y perfiles de acceso.
- En plataformas donde la integración técnica directa no sea factible, el SIAAF mantendrá un registro informativo de las cuentas y roles asignados.
- La recolección de bitácoras de actividad mantendrá su gestión en cada sistema correspondiente. Sin embargo, las bases de datos de cada aplicación deberán mantener actualizados sus registros técnicos de usuarios y roles activos para concordar con la información centralizada o reportada en el SIAAF.

#### **4.5. Acceso físico**

La Dirección de Tecnologías de Información (DTI) definirá los perímetros de seguridad para las áreas que albergan activos críticos. El acceso a estas áreas estará restringido exclusivamente al personal técnico autorizado cuya función laboral así lo exija, aplicando el principio de "menor privilegio".

El Centro de Datos Institucional y los nodos de red distribuidos en las facultades se consideran áreas de alta seguridad, su acceso está restringido al personal autorizado por la DTI. Cualquier ingreso de personal no perteneciente a la DTI (incluyendo otros funcionarios de la UNL o proveedores) deberá contar con una autorización previa y estará supervisado por personal de la DTI durante su permanencia.

El ingreso al Centro de Datos Institucional deberá estar protegido por un esquema de autenticación física robusto, que incluya controles biométricos y/o tarjetas de proximidad. Las bitácoras electrónicas generadas por estos sistemas de control constituyen evidencia digital de auditoría de carácter oficial.

#### **4.6. 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                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Segregación de funciones</b> | Principio fundamental de control interno y seguridad que consiste en dividir las responsabilidades operativas y administrativas entre diferentes personas o roles. Su objetivo es evitar que un solo individuo tenga el control total sobre una transacción crítica (por ejemplo, solicitar, aprobar y crear un usuario) o que el personal de desarrollo tenga acceso de modificación a los entornos de producción, reduciendo así el riesgo de fraude, errores o uso indebido. |
| <b>Usuarios institucionales</b> | Miembros de la comunidad universitaria (autoridades, personal administrativo, trabajadores, docentes y estudiantes) que mantienen un vínculo formal con la Universidad Nacional de Loja y a quienes se les asigna una identidad digital oficial y credenciales para acceder a la red y a las plataformas tecnológicas.                                                                                                                                                          |
| <b>Inventario de usuarios</b>   | Registro centralizado, auditable y actualizado que detalla todas las cuentas de acceso vigentes e inactivas en los sistemas y aplicativos de la UNL. Este inventario documenta el estado de la cuenta, los roles asignados y el nivel de privilegios, facilitando las auditorías de seguridad.                                                                                                                                                                                  |
| <b>Gestión de usuarios</b>      | Proceso técnico y administrativo que abarca el ciclo de vida completo de una identidad digital institucional. Comprende los procedimientos de alta (creación), modificación (cambio de roles o perfiles) y baja (desactivación o revocación) de accesos, ejecutados centralmente a través del módulo de seguridad informática del SIAAF.                                                                                                                                        |
| <b>Solicitud de acceso</b>      | Requerimiento formal y documentado gestionado mediante el Sistema de Servicios de TI + Asistente IA, mediante el cual se pide la habilitación de permisos lógicos o físicos para un usuario. Este requerimiento incluye las firmas de responsabilidad correspondientes y la aceptación previa del Acuerdo de Confidencialidad.                                                                                                                                                  |
| <b>Data Breaches</b>            | Incidente de seguridad cibernética en el que información confidencial, protegida o sensible (como bases de datos de                                                                                                                                                                                                                                                                                                                                                             |

|                                            |                                                                                                                                                                                                                                                                                                                                             |
|--------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                            | credenciales, correos y contraseñas) es accedida, expuesta o robada por personas no autorizadas.                                                                                                                                                                                                                                            |
| <b>Superusuario</b>                        | Cuentas con máximos privilegios, propias de los sistemas informáticos, bases de datos, aplicaciones web y servidores, que poseen la capacidad técnica de alterar configuraciones críticas y evadir restricciones de seguridad. Su uso debe ser estrictamente controlado, trazable y limitado a personal especializado autorizado.           |
| <b>Clave Pública (PKI)</b>                 | Arquitectura y conjunto de políticas de seguridad criptográfica basada en un sistema de llaves asimétricas (una llave pública compartida y una llave privada secreta). En la UNL, se emplea como el estándar obligatorio de autenticación sin contraseñas para administrar servidores de manera remota y segura a través del protocolo SSH. |
| <b>Inicio de sesión único (SSO)</b>        | 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.                                                                                                     |
| <b>Doble Factor de Autenticación (2FA)</b> | 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.         |

## 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 4.2, 4.3 y 4.5.
- 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                                                                                                                                                                                                  |
|---------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Elaborado por:</b>                                                                       | Ing. Juan Carlos Riofrío Herrera<br>OFICIAL DE SEGURIDAD DE LA<br>INFORMACIÓN (OSI)    | <br>Validar únicamente en FirmaEC.<br>Firmado electrónicamente por:<br><b>JUAN CARLOS RIOFRIO<br/>HERRERA</b>       |
| <b>Revisado por:</b>                                                                        | Ing. Jhon Alexander Calderón Sanmartín<br>DIRECTOR DE TECNOLOGÍAS DE LA<br>INFORMACIÓN | <br>Validar únicamente en FirmaEC.<br>Firmado electrónicamente por:<br><b>JHON ALEXANDER<br/>CALDERON SANMARTIN</b> |
| <b>Aprobado:</b><br><br><b>*Comité de<br/>Seguridad de la<br/>Información<br/>(CSI-UNL)</b> | Ing. Magda Cecilia Salazar González<br>DIRECTORA DE PLANIFICACIÓN Y<br>DESARROLLO      | <br>Validar únicamente en FirmaEC.<br>Firmado electrónicamente por:<br><b>MAGDA CECILIA<br/>SALAZAR GONZALEZ</b>   |

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