



Universidad
Nacional
de Loja

Dirección de
Tecnologías de Información

[POLÍTICA]

POLÍTICA DE RESPALDOS DE INFORMACIÓN

Versión 26.08

Agosto 2026

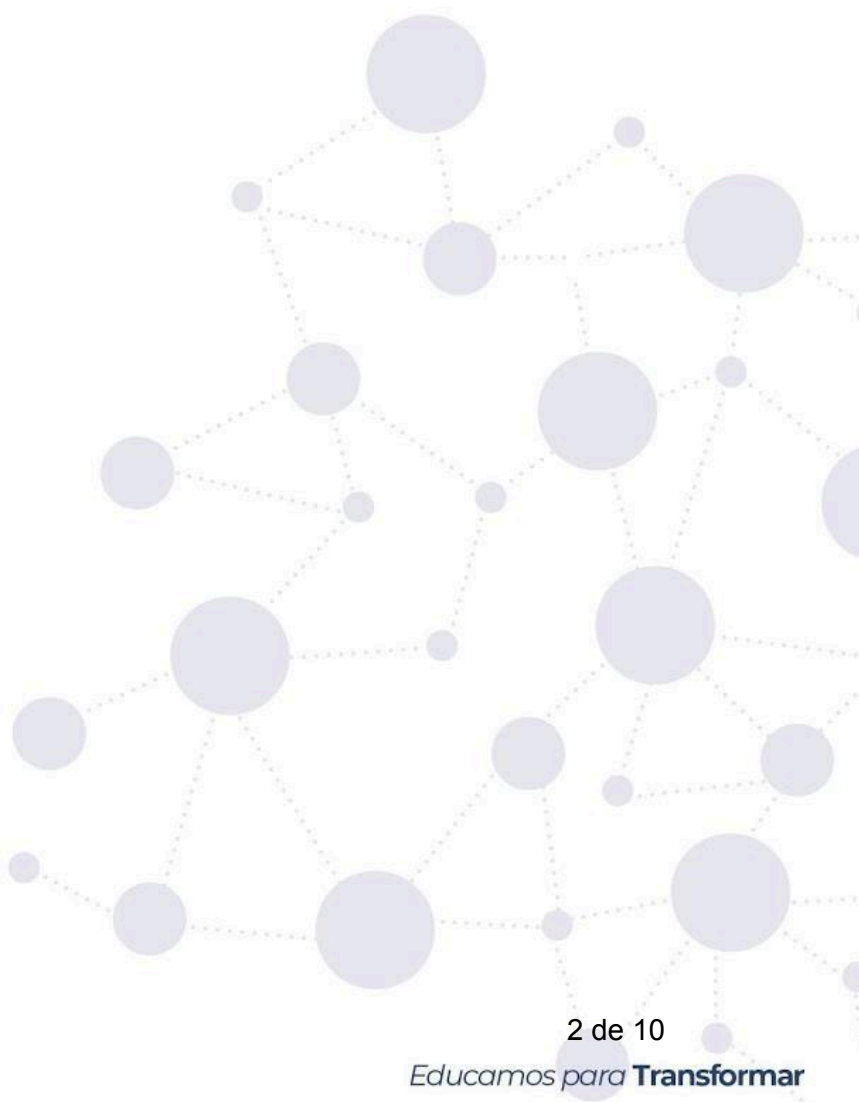
1 de 10

Educamos para **Transformar**



HISTORIAL DE CAMBIOS

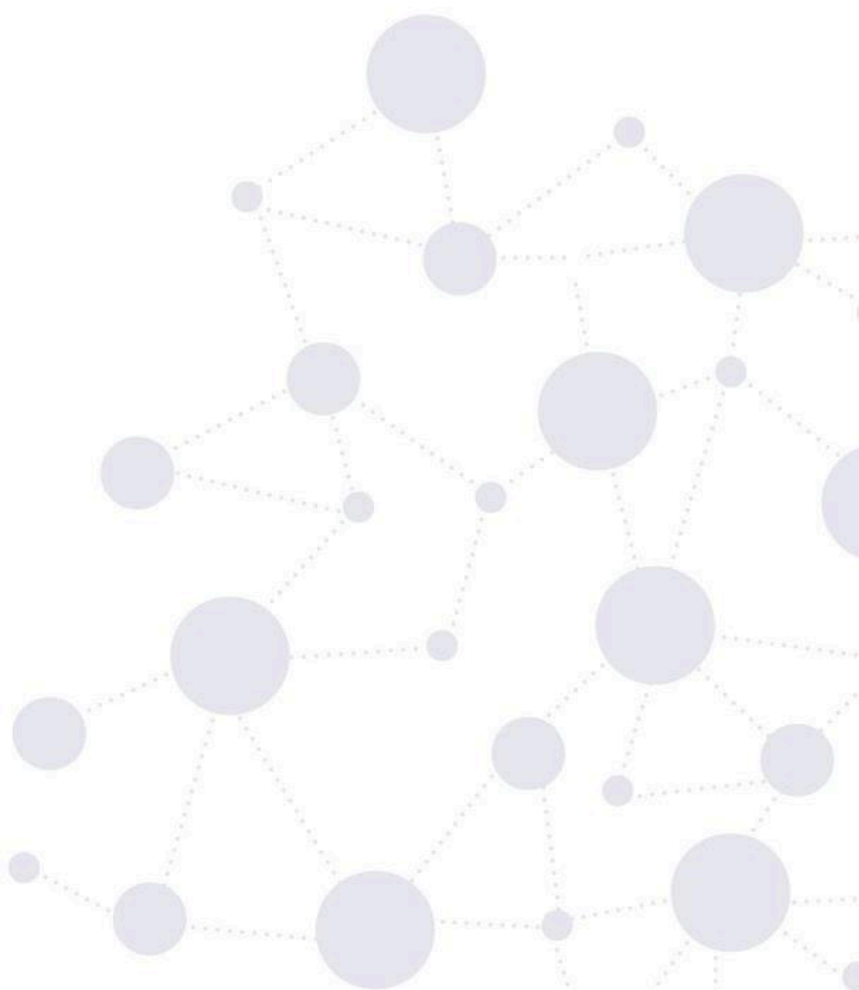
Versión	Fecha	Responsable	Descripción de la modificación
26.08	13/08/2026	Ing. Juan Carlos Riofrío Herrera	Documento inicial





CONTENIDOS

1. Objetivo	4
2. Alcance	4
3. Política	4
4. Lineamientos de la política	4
4.1. Copias de seguridad	4
4.2. Fuentes de información a respaldar	5
4.3. Tipos de respaldo	6
4.4. Priorización y uso eficiente de la nube institucional	7
4.4.1. Asignación de espacio en la nube institucional	8
4.5. Validez y gestión del documento	9
5. Glosario de términos	9
6. Documentos de Referencia	9
7. Firmas de responsabilidad	10



1. Objetivo

Establecer los lineamientos, controles y directrices técnicas y administrativas para la generación, resguardo, verificación y recuperación de las copias de seguridad de los activos de información, sistemas y configuraciones de la Universidad Nacional de Loja; con el fin de garantizar la integridad, disponibilidad y confidencialidad de la información institucional, asegurar la continuidad operativa de las funciones sustantivas (docencia, investigación y vinculación) y proteger los datos personales de la comunidad universitaria ante incidentes de ciberseguridad, fallas tecnológicas o desastres, en cumpliendo con la normativa legal vigente.

2. Alcance

La presente política es de cumplimiento obligatorio para la comunidad universitaria y terceros, conforme al alcance y los usuarios definidos en la Política de Seguridad de la Información. Aplica a todos los activos de información (datos, software y configuraciones) propiedad o bajo custodia de la Universidad Nacional de Loja (UNL), que sean procesados en su infraestructura tecnológica o en servicios externos contratados

3. Política

La Universidad Nacional de Loja declara su compromiso con la confidencialidad, integridad y disponibilidad de la información institucional. Es política de la UNL garantizar que todos los datos críticos, configuraciones de infraestructura y datos personales administrados por la institución cuenten con copias de seguridad actualizadas, cifradas y almacenadas en ubicaciones seguras, que permitan su recuperación oportuna ante desastres naturales, fallas de hardware/software, ciberataques o errores humanos, asegurando la resiliencia y la continuidad de las funciones sustantivas y administrativas de la universidad.

4. Lineamientos de la política

4.1. Copias de seguridad

La Dirección de Tecnologías de Información (DTI) debe realizar copias de seguridad periódicas de la información soportada por la infraestructura tecnológica y sistemas informáticos institucionales críticos, garantizando la recuperación y continuidad de las funciones sustantivas de la UNL ante desastres naturales, fallos u otra forma de error.

Se debe aplicar la regla 3-2-1: Al menos tres (3) copias de los datos, en dos (2) medios diferentes, con una (1) copia inmutable fuera de las instalaciones principales de la UNL.

La DTI, en coordinación con los especialistas de Sistemas de Información e Infraestructura Tecnológica deben crear y almacenar la documentación completa de procedimientos o guías de recuperación (Generación de copias, desarrollo de pruebas, restauración de respaldos, inventario y bitácora de respaldos) asociados con los activos respaldados.

Todas las copias de seguridad que contengan datos personales o financieros deben ser cifradas durante su generación y almacenamiento.

El acceso a los medios de respaldo está restringido exclusivamente al personal técnico autorizado por la DTI.

Todo dispositivo de almacenamiento masivo (Discos externos, memorias flash, cintas, otros) utilizados para el resguardo de información institucional de la UNL, debe permanecer bajo estricta custodia física en las áreas autorizadas del Centro de Datos o dependencias administrativas. Es responsabilidad del custodio del activo que se mantengan protegidos contra riesgos ambientales, pérdida o acceso no autorizado por parte de terceros.

La documentación de los sistemas debe protegerse del acceso no autorizado (esto no incluye los manuales genéricos que se suministran con el software). Se debe aplicar un control de versiones efectivo a toda la documentación y su almacenamiento.

Los medios de almacenamiento que ya no sean necesarios deben eliminarse de forma segura, particularmente cuando se trata de información de identificación personal. Algunos mecanismos de eliminación segura comprenden:

- Formato a bajo nivel (para reutilización)
- Destrucción: por ejemplo a través de golpes con martillo, partirlo físicamente. Antes de desecharlos se debe realizar el proceso administrativo correspondiente.

4.2. Fuentes de información a respaldar

La información susceptible de respaldo se encuentra categorizada de la siguiente forma:

- Servidores físicos y virtuales, incluye bases de datos, código fuente, archivos de configuración, aplicaciones, instaladores, otros que se considere relevante.
- Equipos de comunicación y transmisión de datos, incluye archivos de configuración y/o logs.
- Documentación institucional individual y colaborativa.

4.3. Tipos de respaldo

Con el objetivo de estandarizar la protección de la información en la Universidad Nacional de Loja (UNL) y garantizar la continuidad operativa de sus funciones sustantivas, se establece la presente directriz técnica. Este documento delimita las responsabilidades de ejecución y promueve el principio de corresponsabilidad en la comunidad universitaria para salvaguardar los datos alojados en la infraestructura tecnológica, sistemas de información críticos y los dispositivos de usuario final, en estricto apego a la normativa vigente.

Para la gestión de la información, se definen los siguientes métodos de copia de seguridad:

- **Respaldo completo o Total:** Considera toda la información comprendida en el servidor o equipo de usuario final.
- **Respaldo Incremental:** Se respaldarán los archivos creados a diario.
- **Respaldo Diferencial:** Se respaldarán todos los archivos modificados y creados en la semana.

Estos métodos de copias de seguridad serán usados según la siguiente tabla, sin limitarse a medidas adicionales según se requiera:

Tabla 1. Clasificación y tipo de respaldos

Categoría / Fuente de Información	Elementos específicos a respaldar	Tipo de respaldo a Aplicar	Responsabilidad de ejecución
Servidores Virtuales	Bases de datos, aplicaciones, código fuente, archivos de configuración, instaladores de sistemas, servicios desplegados en la infraestructura virtualizada y otros	Completo e incremental: Combinación programada para optimizar los recursos de almacenamiento y los tiempos de recuperación.	Dirección de Tecnologías de Información (DTI)

	que se consideren críticos.		
Equipos de Comunicación y Transmisión de Datos	Archivos de configuración de red (routers, switches, firewalls) y registros de eventos (logs) de la infraestructura de conectividad.	Completo e incremental: Combinación programada para optimizar recursos de almacenamiento y tiempos de recuperación. Completo (Por evento): Ejecución obligatoria e inmediata luego de cada cambio, actualización o modificación técnica realizada en los equipos.	Administradores de red (DTI) / contratistas de soporte
Equipos de usuario final (personal administrativo y docentes)	Documentación institucional (individual y colaborativa), ofimática, material académico y archivos de gestión diaria.	A elección del funcionario: De libre elección del usuario propietario de la información, quien será el responsable absoluto sobre la gestión, resguardo y disponibilidad de la misma.	Autoridades, Docentes y Personal Administrativo.

Para facilitar el cumplimiento de esta responsabilidad en los equipos de usuario final, la UNL proporciona y recomienda el uso de los repositorios oficiales en la nube institucional. Cada funcionario es responsable exclusivo de garantizar que su documentación institucional se guarde y sincronice correctamente utilizando estas herramientas tecnológicas provistas por la institución.

4.4. Priorización y uso eficiente de la nube institucional

Con el fin de garantizar la sostenibilidad del Campus Inteligente y evitar el colapso de las cuotas de almacenamiento, la UNL prioriza el uso de repositorios en la nube exclusivamente para documentación institucional de tipo documental y ofimático.

Queda restringido el uso de cuentas institucionales para el almacenamiento masivo de archivos multimedia (video y audio) que no cuenten con una justificación técnica.

Las grabaciones de clases deberán ser gestionadas bajo criterios de compresión, temporalidad y depuración semestral, instando a los docentes y servidores a evitar la duplicidad de archivos y la acumulación de información no esencial que comprometan la disponibilidad del servicio para la comunidad universitaria.

4.4.1. Asignación de espacio en la nube institucional

El almacenamiento provisto en la nube institucional es un recurso tecnológico cuyo propósito es estrictamente académico, investigativo, de vinculación y de gestión administrativa. Por consiguiente, queda expresamente prohibido su uso para el almacenamiento de información de carácter personal, entretenimiento o cualquier otro fin que no esté alineado con las funciones sustantivas institucionales de la UNL.

Debido a que la capacidad general de almacenamiento en la nube institucional es limitada, se establecen cuotas máximas por usuario. Esta medida técnica tiene la finalidad de optimizar la infraestructura, evitar la saturación del servicio y garantizar que toda la comunidad universitaria disponga de un acceso equitativo, continuo y eficiente a esta herramienta.

Con base en lo anterior, el espacio de almacenamiento se asignará de manera estandarizada, categorizando a los usuarios según su estamento universitario de la siguiente manera:

- Estudiantes: 15 GB
- Personal Docente: 150 GB
- Personal Administrativo: 100 GB
- Trabajadores: 15 GB
- Cuentas Departamentales: 300 GB (O asignación bajo demanda justificada)

Excepcionalmente, se podrá extender el espacio asignado a las cuentas institucionales que superen su límite. Para ello, el usuario responsable deberá presentar la debida justificación funcional que motive el requerimiento. Toda solicitud estará sujeta a un análisis técnico y documental previo por parte de la DTI. Este análisis

determinará la necesidad real y operativa de aumentar el espacio, o en su defecto, emitirá una recomendación técnica indicando la obligatoriedad de realizar una depuración, compresión o eliminación de la información almacenada.

4.5. 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.

5. Glosario de términos

Término	Definición
Información a respaldar	Cualquier documento, archivo, equipo de cómputo o sistema que contenga datos de valor para las actividades diarias y el funcionamiento de la universidad.
Cifrado de datos	Consiste en transformar los datos legibles en un código secreto para que solo las personas con la clave correcta puedan leerlos, protegiendo así los datos sensibles.
Copia de seguridad (Backup)	Un duplicado exacto de la información importante. Sirve como un salvavidas para recuperar los datos originales si estos se pierden, se borran por accidente, sufren un daño o un ataque informático.
Nube Institucional	Es el espacio de almacenamiento en internet (Google Drive) que la universidad provee para guardar y sincronizar de forma segura documentos académicos y administrativos, sin depender de la memoria física de una sola computadora.
Regla 3-2-1	Una estrategia de prevención fundamental que consiste en tener tres (3) copias de los datos, guardadas en dos (2) tipos de medios diferentes (ej. un servidor y un disco externo), y mantener al menos una (1) de ellas fuera de las instalaciones principales.
Restauración	Es el proceso de "traer de vuelta" o recuperar los datos desde una copia de seguridad hacia la computadora o sistema original, para que todo vuelva a funcionar con normalidad tras un incidente.

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) ítem 4.13
- 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.