Artículo 28°. Autoevaluación y Mejora Continua

La unidad responsable del Repositorio Institucional realizará autoevaluación anual sistemática utilizando la Lista de Verificación de Criterios para la Evaluación de Repositorios Institucionales incluida en la Guía ALICIA como herramienta base, complementada con estándares internacionales reconocidos como los criterios de OpenDOAR, las directrices de OpenAIRE y las mejores prácticas documentadas por la Confederación de Repositorios de Acceso Abierto (COAR) cuando sea apropiado para fortalecer aspectos específicos del repositorio

---

Artículo 29°. Preservación Digital a Largo Plazo

La Universidad Nacional de Juliaca asume el compromiso institucional formal e irrevocable de preservar a largo plazo todos los contenidos depositados en su Repositorio Institucional, reconociendo que la preservación digital constituye una responsabilidad fundamental hacia la comunidad científica, la sociedad y las futuras generaciones que dependerán del acceso continuo a este patrimonio académico y científico para el avance del conocimiento.

Asignación de Recursos para Preservación

La institución asignará recursos humanos, tecnológicos y financieros específicos y suficientes para garantizar la sostenibilidad de las actividades de preservación digital a largo plazo, incluyendo personal especializado con conocimientos técnicos actualizados en preservación digital, gestión de repositorios, estándares internacionales y mejores prácticas emergentes en el campo, asegurando capacitación continua y desarrollo profesional de estos especialistas.

Se asegurará presupuesto anual recurrente específicamente asignado a actividades de preservación digital, no como partida residual sino como línea presupuestaria explícita que reconozca la naturaleza continua y permanente de esta responsabilidad institucional, cubriendo costos de infraestructura, licencias de software especializado, servicios de consultoría técnica, capacitación de personal y actualización tecnológica. Se promoverá la participación activa en redes, consorcios y alianzas de preservación digital como MetaArchive Cooperative, Digital Preservation Network, o iniciativas regionales similares cuando estén disponibles y sean apropiados para el contexto institucional, permitiendo compartir recursos, conocimientos y responsabilidades de preservación con otras instituciones.

Estrategias Técnicas de Preservación

El repositorio implementará estrategias de preservación fundamentadas en estándares internacionales reconocidos y validados por la comunidad global de preservación digital, adoptando el modelo de referencia OAIS (Open Archival Information System, ISO 14721:2012) como marco conceptual que guíe la arquitectura funcional del repositorio y defina los procesos esenciales de preservación.

Conforme al modelo OAIS, el repositorio implementará procesos rigurosos de ingesta validada de contenidos que verifiquen la completitud, integridad y conformidad técnica de los paquetes de información antes de su aceptación definitiva en el repositorio, rechazando depósitos defectuosos o incompletos; almacenamiento seguro con múltiples copias de respaldo mantenidas en medios y ubicaciones diferentes aplicando la regla 3-2-1 (tres copias, dos medios diferentes, una ubicación externa) como mínimo estándar de seguridad; y gestión exhaustiva de metadatos administrativos,

descriptivos, técnicos y de preservación incluyendo la implementación del estándar PREMIS (PREservation Metadata: Implementation Strategies) que documenta objetos digitales, eventos, agentes y derechos asociados a los procesos de preservación.

Artículo 30°. Seguridad y Sostenibilidad

La UNAJ implementará medidas técnicas robustas para garantizar la seguridad, integridad y disponibilidad de los contenidos y datos del Repositorio Institucional, siendo responsabilidad de la oficina de tecnologías de la información en coordinación con la unidad responsable del repositorio el diseño, implementación y mantenimiento de estos controles de seguridad.

En materia de seguridad de datos, se aplicará encriptación de datos en tránsito mediante protocolos HTTPS/TLS para proteger la información durante su transmisión por la red, encriptación de datos en reposo cuando contengan información sensible o confidencial, control de acceso basado en roles para administradores y gestores del repositorio asignando privilegios mínimos necesarios según funciones, autenticación multifactor para accesos privilegiados al sistema, generación de registros de auditoría de acceso a datos restringidos que permitan rastrear consultas y descargas, y respaldos encriptados almacenados en ubicaciones seguras geográficamente dispersas que garanticen la recuperación de información ante eventos adversos.

Para la protección contra amenazas, se implementarán firewalls y sistemas de detección y prevención de intrusiones que monitoreen el tráfico de red, mecanismos de protección contra ataques de denegación de servicio que puedan afectar la disponibilidad del repositorio, aplicación regular y oportuna de actualizaciones de seguridad del software del repositorio y sus componentes, evaluaciones periódicas de vulnerabilidades realizadas por personal especializado o entidades certificadas, un plan de respuesta a incidentes de seguridad que establezca procedimientos claros para identificación, contención, erradicación y recuperación ante eventos de seguridad, y protocolos de notificación a afectados cuando corresponda conforme a la normativa de protección de datos personales.

La preservación segura a largo plazo se garantizará mediante múltiples copias de respaldo, verificación periódica de integridad de archivos mediante sumas de verificación criptográficas (checksums) que detecten corrupciones o alteraciones no autorizadas, migración planificada de formatos obsoletos a formatos vigentes manteniendo la integridad del contenido y sus metadatos, documentación detallada de procedimientos de seguridad y preservación digital que permita continuidad operativa ante cambios de personal, y auditorías periódicas del cumplimiento de estándares de seguridad y preservación digital reconocidos internacionalmente.

La unidad responsable del repositorio establecerá un cronograma de revisión y actualización de las medidas de seguridad para adaptarse a las amenazas emergentes y a las mejores prácticas en evolución. Cualquier incidente de seguridad que afecte o pueda afectar la confidencialidad, integridad o disponibilidad de los contenidos del repositorio será documentado e investigado, y se tomarán las acciones correctivas necesarias para prevenir su recurrencia.