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.

Artículo 38°. Infraestructura Tecnológica

La Universidad Nacional de Juliaca garantizará la provisión y mantenimiento de infraestructura tecnológica robusta, confiable y escalable para el funcionamiento apropiado y sostenible del Repositorio Institucional.

Selección de la Plataforma de Software

La plataforma tecnológica del repositorio será seleccionada considerando su conformidad con estándares nacionales establecidos por CONCYTEC y protocolos internacionales de

interoperabilidad como OAI-PMH; preferencia por software libre o de código abierto como DSpace, EPrints o plataformas similares que faciliten personalización, reducción de costos de licenciamiento y sostenibilidad a largo plazo; capacidad de escalamiento técnico y funcional para albergar el crecimiento futuro de colecciones sin degradación de rendimiento; facilidad de uso e interfaces intuitivas tanto para depositantes como para usuarios finales; solidez y actividad de la comunidad internacional de desarrollo que garantice continuidad, actualizaciones regulares y disponibilidad de soporte técnico; y compatibilidad técnica con otros sistemas institucionales existentes como plataformas de gestión académica, sistemas de autenticación y directorios institucionales.

Infraestructura de Servidores y Almacenamiento

La institución garantizará capacidad suficiente de almacenamiento para albergar las colecciones actuales y proyectadas con holgura apropiada que permita crecimiento sin requerir ampliaciones urgentes; sistemas redundantes de almacenamiento con respaldos automatizados diarios incrementales y semanales completos, almacenados en ubicaciones físicas geográficamente diferentes para protección contra desastres; conexión a internet de alta velocidad, estabilidad y disponibilidad que garantice accesibilidad continua al repositorio desde ubicaciones nacionales e internacionales; medidas robustas de seguridad informática incluyendo firewalls configurados apropiadamente, sistemas de detección y prevención de intrusiones, certificados SSL/TLS actualizados para encriptación de comunicaciones, y aplicación oportuna de actualizaciones de seguridad.

Se implementarán sistemas de monitoreo automatizado que permitan detección temprana de problemas técnicos como caídas de servicio, degradación de rendimiento, llenado de espacios de almacenamiento o intentos de intrusión, con alertas automáticas al personal responsable; y planes documentados de recuperación ante desastres que especifiquen procedimientos detallados de restauración del servicio en caso de fallas graves, asignación de responsabilidades, tiempos objetivo de recuperación, y contactos de personal clave y proveedores.

Actualización y Mantenimiento de la Plataforma

La institución mantendrá actualizada la plataforma del repositorio aplicando oportunamente actualizaciones de seguridad críticas, parches correctivos de errores y nuevas versiones estables del software que incorporen mejoras funcionales o de rendimiento, siempre considerando la necesidad de realizar pruebas apropiadas en ambientes de desarrollo o prueba antes de aplicar actualizaciones en el ambiente de producción para evitar interrupciones de servicio o pérdida de funcionalidad, y documentando apropiadamente todos los cambios realizados en la configuración del sistema, versiones de software instaladas y procedimientos aplicados para facilitar diagnóstico de problemas futuros y garantizar continuidad del conocimiento técnico ante rotación de personal.