

Lineamientos de preservación digital, seguridad de la información y protocolo de interoperabilidad

Universidad Católica Luis Amigó

Con el compromiso de promover la excelencia académica y la gestión del conocimiento, la Universidad Católica Luis Amigó establece los presentes lineamientos de Preservación Digital y Seguridad de la Información. Estos constituyen el marco de referencia obligatorio para garantizar la protección, integridad y disponibilidad de los activos digitales que integran el patrimonio intelectual de la institución, incluidos los disponibles en las plataformas Open Journal Systems (OJS) y Open Monograph Press (OMP).

Este ecosistema garantiza que la producción editorial de la Universidad permanezca accesible y protegida frente a incidentes técnicos o ciberamenazas, asegurando la continuidad institucional y el acceso abierto al conocimiento.

Primero. Infraestructura tecnológica

La Universidad Católica Luis Amigó adopta un modelo tecnológico híbrido que integra infraestructura local (*on-premise*), servicios en nube privada y en nube pública. En estos entornos, la protección de la información institucional constituye una responsabilidad indelegable de la Universidad.

El Departamento de Infraestructura y Desarrollo Tecnológico para la Educación garantiza que los mecanismos de seguridad tecnológica se gestionen de manera articulada, coherente y proporcional al nivel de riesgo, asegurando que los controles implementados respondan a criterios de continuidad operativa, confidencialidad, integridad y disponibilidad de la información.

En los servicios en nube pública se aplica el principio de responsabilidad compartida, velando por la correcta configuración, administración de accesos y protección de los datos institucionales, sin perjuicio de las obligaciones contractuales asumidas por los proveedores tecnológicos.

La adopción de nuevas plataformas, servicios digitales o soluciones en la nube requiere validación previa del Departamento de Infraestructura y Desarrollo Tecnológico para la Educación, para asegurar que cumplan con los lineamientos institucionales de arquitectura, seguridad y gobierno tecnológico.

Segundo. Seguridad de la información

La infraestructura tecnológica institucional está respaldada por mecanismos de protección, como:

- Firewall de nueva generación.
- Segmentación lógica de red.
- Control de acceso a la red.
- Soluciones avanzadas de protección para equipos y servidores.
- Esquemas de copias de respaldo con características de inmutabilidad.

Estos controles se integran dentro de un marco formal de gobierno de la seguridad de la información.

La seguridad es entendida como una responsabilidad compartida. En este sentido, la Universidad promueve espacios de sensibilización y buenas prácticas en ciberseguridad, fomentando el uso consciente, ético y responsable de los recursos tecnológicos institucionales.

Tercero. Gestión de incidentes de seguridad

Todo miembro de la comunidad académica deberá reportar de manera inmediata cualquier evento que pueda comprometer la seguridad de la información al correo institucional: ciberseguridad@amigo.edu.co

El reporte oportuno permite activar los protocolos internos de análisis, contención y mitigación, contribuyendo a la protección de los activos digitales institucionales.

Cuarto. Preservación digital (respaldo y continuidad)

La Universidad garantiza la realización periódica de copias de respaldo de la información crítica y promueve el fortalecimiento progresivo de su capacidad de recuperación ante eventos que puedan afectar la continuidad institucional.

Actualmente, el esquema de respaldos incluye:

- *Backups* incrementales diarios.
- Copias de seguridad semanales.
- Copias de seguridad mensuales.

Este modelo permite la recuperación de información ante incidentes técnicos, fallos del sistema o eventos no previstos, asegurando la preservación y disponibilidad continua de los contenidos digitales institucionales, incluidos los recursos editoriales.

Quinto. Ecosistema de repositorios y visibilidad

El Repositorio Institucional es una plataforma para el almacenamiento, difusión, preservación y gestión integral de la producción académica y editorial. Actualmente opera sobre DSpace 7.6, con proceso de mejora hacia DSpace-CRIS, ampliando capacidades de gestión de entidades de investigación conforme a estándares internacionales.

El modelo de preservación digital en este repositorio, se fundamenta en:

- Organización estructurada en comunidades y colecciones.
- Archivo histórico completo y permanente de publicaciones.
- Identificadores persistentes y URLs estables.
- Control de integridad de datos en procesos de actualización.
- Copias de seguridad periódicas de base de datos y archivos.

En cuanto a la interoperabilidad y estándares internacionales, el repositorio opera bajo protocolos internacionales que garantizan su integración con el ecosistema global de información científica:

- Implementación del protocolo OAI-PMH para cosecha de metadatos.
- Cumplimiento de lineamientos de interoperabilidad compatibles con OpenAIRE.
- Soporte para integración con ORCID y sistemas DOI.
- Compatibilidad con principios de acceso abierto y posibilidades de acercamiento a la ciencia abierta.

Estas capacidades permiten visibilidad internacional, trazabilidad de la producción científica y cumplimiento de requerimientos técnicos de los sistemas de indexación.

Complementariamente, la Universidad participa en Consortia Papyrus, repositorio multidisciplinar para la preservación de datos científicos, garantizando:

- Asignación de DOI mediante DataCite.
- Metadatos normalizados.
- Versionamiento y trazabilidad.
- Custodia técnica especializada.

La articulación entre DSpace y Papyrus fortalece el cumplimiento de los principios FAIR (*Findable, Accessible, Interoperable, Reusable*) y consolida la estrategia institucional de acceso abierto.

Sexto. Responsabilidad de los gestores del OJS y OMP

Los editores y equipos técnicos de las plataformas OJS (Open Journal Systems) y OMP (Open Monograph Press) asumen las siguientes responsabilidades para garantizar la integridad del patrimonio digital:

- Administración de usuarios: Aplicar el principio de responsabilidad compartida en la configuración de roles dentro de los sistemas OJS/OMP, asegurando que los permisos de acceso sean proporcionales a las funciones de cada colaborador.
- Validación técnica: Cualquier implementación de nuevos módulos, plugins o integraciones en las plataformas editoriales debe contar con la validación previa del Departamento de Infraestructura y Desarrollo Tecnológico para la Educación, para alinearse con el gobierno tecnológico institucional.