Humanidades digitales, ciberseguridad y preservación del patrimonio cultural: riesgos legales y técnicos de los repositorios digitales

Sección: Artículo
Recibido: 01/05/2026
Aceptado: 29/06/2026
DOI: 10.46530/virtualis.v18i31.497

Digital Humanities, Cybersecurity, and Cultural Heritage Preservation: Legal and Technical Risks of Digital Repositories

Carlos Ramírez Castañeda
Universidad Abierta y a Distancia de México, México
ORCID: 0000-0002-3400-3408
correo: cybercrimemx@hotmail.com

Resumen. Los repositorios digitales se han convertido en el soporte fundamental del patrimonio cultural, académico e histórico de la humanidad. Sin embargo, la transición hacia entornos digitales ha traído consigo una superficie de riesgo que las instituciones custodias (archivos, bibliotecas, museos y universidades) no siempre han sabido dimensionar ni gestionar con la profundidad que el fenómeno exige. Este artículo analiza, desde un enfoque interdisciplinario que articula las humanidades digitales con la ciberseguridad y el derecho, los principales riesgos técnicos y legales que enfrentan los repositorios digitales de patrimonio cultural: ataques de *ransomware*, pérdida de integridad documental, accesos indebidos, obsolescencia de formatos, ausencia de marcos normativos de preservación a largo plazo y deficiencias en la interoperabilidad. Se adopta un diseño metodológico cualitativo basado en revisión documental sistematizada de literatura especializada, análisis de casos emblemáticos de incidentes sobre repositorios culturales y revisión del marco jurídico internacional y mexicano aplicable. Los resultados muestran que la debilidad no reside únicamente en las capas técnicas de los sistemas, sino en la falta de modelos de gobernanza, políticas de seguridad adaptadas

Abstract. Digital repositories have become the fundamental support for the cultural, academic, and historical heritage of humanity. However, the transition to digital environments has brought with it a risk surface that custodial institutions (archives, libraries, museums, and universities) have not always been able to measure or manage with the depth the phenomenon demands. This article analyzes, from an interdisciplinary approach that articulates digital humanities with cybersecurity and law, the main technical and legal risks facing digital repositories of cultural heritage: *ransomware* attacks, loss of documentary integrity, unauthorized access, format obsolescence, absence of normative frameworks for long-term preservation, and deficiencies in interoperability. A qualitative methodological design is adopted, based on a systematized documentary review of specialized literature, analysis of emblematic cases of incidents involving cultural repositories, and a review of the applicable international and Mexican legal framework. The results show that the weakness does not reside solely in the technical layers of the systems, but in the lack of governance models, security policies adapted to the specificity of digital heritage, and specialized

a la especificidad del patrimonio digital y formación especializada en los equipos responsables. Se concluye proponiendo una agenda de política institucional que integre ciberseguridad, derecho y humanidades digitales como condición necesaria para garantizar la preservación y el acceso sostenible al patrimonio cultural en entornos digitales.

Palabras clave: humanidades digitales; ciberseguridad; patrimonio cultural digital; repositorios digitales; preservación digital; riesgos legales.

training for the responsible teams. The article concludes by proposing an institutional policy agenda that integrates cybersecurity, law, and digital humanities as a necessary condition to guarantee the preservation and sustainable access to cultural heritage in digital environments.

Keywords: digital humanities; cybersecurity; digital cultural heritage; digital repositories; digital preservation; legal risks.

Introducción

La pregunta sobre qué significa preservar no es nueva. Durante siglos, las civilizaciones han desarrollado técnicas, instituciones y rituales para proteger aquello que consideran valioso: tablillas de barro, pergaminos, papiros, códices iluminados, registros notariales, partituras, actas gubernamentales, correspondencia diplomática. Cada soporte implicaba sus propias vulnerabilidades: el fuego, la humedad, los insectos, el tiempo, y cada época construyó sus propios sistemas de custodia. La digitalización no ha abolido esa lógica, la ha complejizado hasta un punto que aún no terminamos de dimensionar.

El patrimonio cultural en sus formas digitales ya no es un horizonte futuro: es una realidad operativa que abarca desde los archivos históricos escaneados de las bibliotecas nacionales hasta los acervos sonoros digitalizados de comunidades indígenas, desde los catálogos en línea de los museos hasta los repositorios institucionales de universidades que resguardan tesis, investigaciones y colecciones fotográficas de décadas. En México, el proceso de digitalización de acervos ha avanzado a ritmos desiguales, impulsado por iniciativas como el Programa Nacional Digitalia de la Secretaría de Cultura, el Sistema de Repositorios Abiertos y las plataformas de las grandes bibliotecas universitarias, entre ellas la Biblioteca Nacional de México, el Fondo Reservado y los sistemas UNAM-Digitalia. A nivel global, la Biblioteca Digital Mundial (World Digital Library), impulsada por la UNESCO y la Biblioteca del Congreso de Estados Unidos, y Europeana, el repositorio europeo de patrimonio cultural, se han convertido en referentes sobre las posibilidades (pero también sobre los desafíos), de la preservación digital a escala institucional.

Sin embargo, la transición hacia lo digital ha abierto una superficie de riesgo que las instituciones custodias no siempre han abordado con la profundidad que merece. Cuando un archivo histórico en soporte papel era destruido por un incendio o inundado, el daño era irreversible, pero circunscrito. Cuando un repositorio digital es comprometido por un ataque de *ransomware*, la afectación puede ser simultáneamente masiva, remota, silenciosa y, en los peores escenarios, también irreversible. La diferencia no es solo de escala: es de naturaleza. Los riesgos que enfrenta el patrimonio cultural en entornos digitales combinan vulnerabilidades técnicas (fallos de sistema, ataques cibernéticos, obsolescencia tecnológica), vulnerabilidades jurídicas (vacíos normativos, conflictos de propiedad intelectual, ausencia de marcos de responsabilidad) y vulnerabilidades institucionales (falta de recursos, de formación especializada y de políticas de gobernanza digital).

El presente artículo parte de la convicción de que las humanidades digitales, entendidas como el campo interdisciplinario que articula métodos computacionales y reflexión humanística sobre el conocimiento, la cultura y la memoria, tienen una responsabilidad específica en este debate. No basta con construir repositorios; es necesario pensar con qué lógica se construyen, qué garantías ofrecen, qué marcos normativos los regulan y qué herramientas técnicas y éticas están desplegadas para protegerlos. El diálogo entre humanidades digitales, ciberseguridad y derecho no es un lujo académico: es una condición de posibilidad para que el patrimonio cultural digital sobreviva a las amenazas del presente y sea accesible para las generaciones futuras.

Este problema interesa de manera directa al campo de la comunicación, pues los repositorios digitales de patrimonio cultural no son solo dispositivos de almacenamiento: son infraestructuras de comunicación pública de la memoria, en las que se decide qué bienes culturales circulan socialmente, en qué condiciones de acceso y bajo qué mediaciones técnicas. La preservación y la seguridad de un repositorio determinan, en sentido estricto, la posibilidad misma de que el patrimonio sea comunicado: un acervo cifrado por un ataque, corrompido por la degradación silenciosa de los datos o vuelto ilegible por la obsolescencia tecnológica deja de circular, deja de ser consultable y, con ello, deja de cumplir su función comunicativa en la esfera pública. Desde esta perspectiva, la ciberseguridad y la preservación digital no son asuntos meramente técnicos o jurídicos, sino condiciones de la gobernanza comunicativa de los repositorios abiertos y de la infraestructura informacional de la memoria colectiva.

El presente artículo se sitúa, por tanto, en la intersección entre la comunicación pública del patrimonio, las humanidades digitales, la ciberseguridad y el derecho.

Con la premisa anterior, este artículo se orienta por una pregunta principal de investigación: ¿qué riesgos técnicos y legales comprometen la preservación y el acceso sostenible del patrimonio cultural alojado en repositorios digitales, y qué condiciones institucionales se requieren para mitigarlos en el contexto mexicano y latinoamericano? De ella se derivan tres preguntas secundarias:

a) ¿De qué manera se imbrican las dimensiones técnica, jurídica e institucional en cada uno de los riesgos identificados, de modo que no puedan atenderse de forma aislada?
b) ¿Qué vacíos normativos del ordenamiento mexicano dejan sin protección al patrimonio cultural digital, en particular tras la reconfiguración institucional reciente en materia de protección de datos? y
c) ¿Qué papel corresponde a las humanidades digitales en la articulación de respuestas a estos riesgos?

El aporte original del trabajo no reside en describir por separado la preservación digital, la ciberseguridad institucional o el derecho del patrimonio, campos que cuentan con literatura consolidada, sino en proponer su intersección como el espacio analítico desde el cual deben comprenderse y gobernarse los repositorios culturales, con atención específica al contexto mexicano y latinoamericano.

De manera general, el texto se organiza de la siguiente manera. Tras esta introducción, se presenta el apartado de Material y Métodos donde se describe el diseño de la investigación. A continuación, se desarrolla el marco teórico-conceptual que articula los tres campos disciplinarios en cuestión. El cuerpo del artículo analiza sistemáticamente los principales riesgos técnicos y legales de los repositorios digitales, con atención al contexto mexicano y latinoamericano. La sección de resultados y discusión contrasta los hallazgos con la literatura especializada y propone lineamientos de política institucional. Finalmente, las conclusiones sintetizan los aportes del trabajo y trazan las líneas de investigación futura.

Material y métodos

Este trabajo adopta un diseño metodológico cualitativo de carácter teórico-analítico, estructurado sobre tres procedimientos complementarios. El primero es una revisión documental sistematizada de la literatura especializada en humanidades digitales, preservación digital, ciberseguridad de repositorios y marcos jurídicos de protección

del patrimonio cultural. Para ello se consultaron bases de datos como Scopus, Web of Science, ERIC, JSTOR, Dialnet y el repositorio de la *Digital Humanities Quarterly*, priorizando publicaciones de los últimos diez años, aunque integrando referencias fundacionales cuando resulta pertinente para la construcción del marco teórico. Es menester precisar el alcance de esta revisión: no se trata de una revisión sistemática en sentido estricto, con protocolo replicable de tipo PRISMA, sino de una revisión sistematizada y de carácter cualitativo, en la que la selección de fuentes obedeció a criterios de pertinencia temática, calidad de la publicación y relevancia para la construcción del argumento, más que a una pretensión de exhaustividad, se privilegiaron artículos arbitrados, informes de organismos especializados y estándares técnicos reconocidos internacionalmente, descartando fuentes sin respaldo institucional o académico verificable.

Para fortalecer los procedimientos de revisión, la tabla 1 sintetiza las fuentes consultadas, los criterios de búsqueda, los criterios de inclusión y exclusión, así como la finalidad analítica de cada grupo documental. Esta tabla no pretende constituir un protocolo bibliométrico exhaustivo, sino explicitar el proceso de construcción del corpus documental utilizado para el análisis cualitativo y así logre comprenderse el contexto metodológico para la selección de texto.

El segundo procedimiento es el análisis de casos emblemáticos de incidentes que han afectado repositorios digitales culturales o institucionales a nivel global, seleccionados por su relevancia documental, impacto sistémico y capacidad ilustrativa de los distintos vectores de riesgo identificados. La selección de casos no pretende ser exhaustiva, sino representativa de la diversidad de amenazas y contextos: incluye ataques de *ransomware* a instituciones culturales, episodios de pérdida masiva de datos por obsolescencia tecnológica, vulneraciones de acceso no autorizado y conflictos de propiedad intelectual en la digitalización de acervos. Los criterios de inclusión para los incidentes fueron:

a) Que el incidente estuviera documentado en fuentes verificables (prensa especializada, informes institucionales o literatura académica);
b) Que afectara a instituciones de memoria, educativas o gubernamentales con funciones de custodia documental;
c) Que ilustrara con claridad uno de los vectores de riesgo analizados.

Tabla 1
Criterios metodológicos de la revisión documental sistematizada

Componente	Descripción
Bases y repositorios consultados	Scopus, Web of Science, ERIC, JSTOR, Dialnet, Digital Humanities Quarterly, documentos institucionales de UNESCO, NIST, ISO, Library of Congress y legislación mexicana aplicable.
Periodo de búsqueda	Se priorizaron publicaciones de los últimos diez años, sin excluir referencias fundacionales cuando fueran necesarias para explicar modelos técnicos, jurídicos o conceptuales.
Descriptores orientadores	"digital preservation", "digital repositories", "cultural heritage", "cybersecurity", "trusted digital repositories", "OAIS", "PREMIS", "*ransomware*", "archives", "libraries", "patrimonio digital", "repositorios digitales", "protección de datos" y "derechos de autor".
Criterios de inclusión	Publicaciones arbitradas, estándares técnicos, documentos normativos, informes institucionales y casos documentados que permitieran analizar riesgos técnicos, jurídicos o institucionales de repositorios digitales.
Criterios de exclusión	Fuentes sin respaldo académico o institucional verificable, incidentes sin confirmación pública suficiente y documentos no relacionados directamente con preservación digital, ciberseguridad, patrimonio cultural o regulación de repositorios.
Procedimiento de análisis	Lectura temática y triangulación cualitativa de fuentes, organizando los hallazgos en tres dimensiones: técnica, jurídica e institucional.
Finalidad analítica	Construir un marco integrado que permita examinar los riesgos de los repositorios digitales de patrimonio cultural y proponer lineamientos de política institucional.

Se excluyeron incidentes sin confirmación pública o cuya naturaleza técnica no pudiera establecerse con certeza razonable.

El tercer procedimiento es una revisión analítica del marco jurídico internacional y mexicano aplicable a la preservación digital del patrimonio cultural, con énfasis en las

disposiciones sobre protección de datos, propiedad intelectual, depósito legal digital y derecho de acceso a la información. Se analizan instrumentos como la Carta de la UNESCO sobre la Preservación del Patrimonio Digital, el Tratado de Marrakech sobre el acceso a las obras publicadas por personas con discapacidad visual, la Ley Federal del Derecho de Autor mexicana, la Ley General de Archivos y la normativa derivada de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
El análisis se realizó mediante un enfoque de triangulación de fuentes: cada riesgo identificado se examina desde la dimensión técnica, la dimensión jurídica y la dimensión institucional, con el fin de construir una comprensión integrada que trascienda las miradas sectoriales. El artículo no presenta datos empíricos primarios obtenidos a través de trabajo de campo, sino que articula fuentes secundarias especializadas para construir un argumento teórico-analítico orientado a la proposición de lineamientos de política institucional.

Marco teórico-conceptual: tres campos en conversación necesaria

Las humanidades digitales como campo de responsabilidad patrimonial

Las humanidades digitales han transitado, en las últimas tres décadas, de ser un espacio experimental de aplicación de herramientas informáticas a los estudios humanísticos a constituirse en un campo disciplinario con problemas, métodos y debates propios (Burdick et al., 2012; Drucker, 2021; Terras et al., 2016). En su acepción más amplia, refieren al conjunto de prácticas que articulan computación y humanidades para producir conocimiento sobre la cultura, la historia, la lengua, la memoria y el arte. Esta articulación no es meramente instrumental: implica asumir que los métodos digitales transforman los objetos de estudio, generan nuevas preguntas y exigen formas de reflexividad que las humanidades tradicionales no habían necesitado desarrollar.

En el ámbito del patrimonio cultural, las humanidades digitales han aportado prácticas transformadoras: la digitalización de manuscritos medievales, el análisis computacional de corpus literarios, la creación de bases de datos de cerámica arqueológica con sistemas de descripción interoperables, la construcción de ediciones críticas digitales o la georeferenciación de rutas históricas. Sin embargo, este impulso de apertura y democratización del acceso al patrimonio ha estado acompañado de un optimismo tecnológico que en ocasiones ha subestimado los riesgos que la digitalización introduce. Rinehart et al. (2014) advierten que una parte significativa de los proyectos de preservación digital en instituciones pequeñas o medianas suelen iniciar con recursos limitados, sin políticas consolidadas y con dificultades para traducir la capacitación en acciones

sostenidas, asumiendo implícitamente que los datos producidos "estarán ahí" cuando se los necesite. Esta suposición es, como se argumentará en este artículo, una de las mayores vulnerabilidades del patrimonio cultural digital.

La responsabilidad patrimonial de las humanidades digitales no se agota en producir acceso: implica pensar las condiciones de sostenibilidad, seguridad e integridad de los objetos digitales que se crean y custodian. Flanders y Jannidis (2019) han planteado que el cuidado [*stewardship*] de los datos digitales es una obligación ética inseparable de la práctica de las humanidades digitales. Esta perspectiva conecta directamente con los debates de la ciberseguridad y el derecho.

Ciberseguridad como práctica institucional, no como especialidad técnica

Uno de los errores más persistentes en la gestión de riesgos digitales en las instituciones culturales es concebir la ciberseguridad como una responsabilidad exclusiva de los departamentos técnicos de informática. Esta concepción reduce el problema a sus capas de infraestructura y descuida las dimensiones organizacionales, humanas y normativas que en la mayoría de los incidentes documentados resultan ser los vectores de entrada más relevantes. Como señalan Rid y McBurney (2012), la mayor parte de los ataques exitosos contra sistemas institucionales no explotan vulnerabilidades técnicas sofisticadas, sino errores humanos, configuraciones incorrectas y ausencia de protocolos de respuesta.

En el contexto de los repositorios culturales, la ciberseguridad debe entenderse como un conjunto de prácticas institucionales que abarcan desde la arquitectura técnica del sistema hasta la formación del personal, los protocolos de acceso, las políticas de respaldo, los planes de respuesta ante incidentes y los marcos de evaluación continua de riesgos. El National Institute of Standards and Technology (NIST) de Estados Unidos proporciona, a través de su Cybersecurity Framework, una de las referencias más utilizadas internacionalmente para estructurar este tipo de aproximación integral (NIST, 2024). En su versión 2.0, publicada en febrero de 2024, el marco organiza las prácticas en torno a seis funciones: gobernar, identificar, proteger, detectar, responder y recuperar. La incorporación de la función gobernar como eje rector resulta especialmente pertinente para las instituciones culturales, pues sitúa la ciberseguridad como una responsabilidad de gobernanza institucional y no como una tarea exclusivamente técnica, en línea con el argumento central de este artículo. Además, la versión 2.0 amplía explícitamente su alcance a organizaciones de todo tipo y tamaño, lo que facilita su adaptación por archivos, bibliotecas y museos de recursos limitados.

Desde la perspectiva de la preservación digital, la ciberseguridad se entrecruza con el concepto de autenticidad: garantizar que un objeto digital no ha sido alterado, ni por actores maliciosos ni por fallos técnicos, desde su creación hasta el momento en que se accede a él es una condición fundamental de la preservación (Lynch, 1999). Esta dimensión conecta la ciberseguridad con los marcos teóricos de la archivística y la bibliotecología digital, y sitúa la integridad documental como un valor transversal que no puede delegarse únicamente a los sistemas informáticos.

El derecho ante el patrimonio cultural digital: un marco en construcción

El derecho ha respondido a la digitalización del patrimonio cultural de manera fragmentada y, con frecuencia, tardía. Los marcos normativos existentes fueron diseñados en gran medida para objetos físicos y categorías jurídicas consolidadas, el libro, el archivo, la obra de arte, que no se ajustan con precisión a las especificidades de los objetos digitales: su reproducibilidad infinita, su dependencia de infraestructuras tecnológicas cambiantes, la multiplicidad de capas de autoría y derechos que pueden superponerse en un solo objeto, o la tensión permanente entre el acceso abierto y la protección de los derechos de propiedad intelectual (Besek et al., 2008; Directiva (UE) 2019/790).

En el plano internacional, la UNESCO (2003), mediante la Carta sobre la preservación del patrimonio digital, constituyó uno de los primeros instrumentos de referencia específicamente orientados a los objetos digitales, al reconocer que el patrimonio digital es frágil, que su preservación requiere esfuerzos concertados y que los Estados tienen responsabilidades específicas en este campo. Sin embargo, la Carta carece de fuerza vinculante y sus disposiciones no han derivado en marcos normativos nacionales con suficiente especificidad técnica y jurídica.

En México, la Ley General de Archivos de 2018 introdujo disposiciones relevantes sobre la preservación de documentos electrónicos en el ámbito público, estableciendo principios de conservación, accesibilidad e integridad que se extienden, en principio, a los acervos digitales de las instituciones del Estado. La Ley Federal del Derecho de Autor (LFDA) regula los derechos sobre las obras digitalizadas, pero genera tensiones con las prácticas de digitalización masiva de acervos que las instituciones culturales desarrollan bajo la excepción de uso cultural o educativo. Estas tensiones se vuelven especialmente complejas cuando los materiales digitalizados son objeto de acceso abierto, de reutilización para proyectos de humanidades digitales o de minería de datos (Directiva (UE) 2019/790).

Tres literaturas en tensión: hacia un esquema analítico integrado

Los tres campos reseñados no dialogan de manera espontánea; más bien operan como cuerpos de literatura paralelos que rara vez se interpelan. La literatura sobre preservación digital ha producido estándares técnicos robustos, como el modelo OAIS (ISO 14721:2012), el estándar de metadatos de preservación PREMIS (PREMIS Editorial Committee, 2015) o el marco de auditoría de repositorios confiables ISO 16363:2012, pero tiende a tratar la ciberseguridad como un asunto periférico y la dimensión jurídica como un dato de contexto. La literatura de ciberseguridad institucional ofrece marcos maduros de gestión del riesgo (NIST, 2024; ISO/IEC 27001:2022), pero no incorpora las particularidades del patrimonio cultural: la irreversibilidad de la pérdida, el valor simbólico de los objetos o el deber público de custodia. La literatura de humanidades digitales, por su parte, ha teorizado con solidez la ética del cuidado de los datos y los principios CARE para la gobernanza de datos de comunidades (Carroll et al., 2020), pero ha subvalorado la dimensión técnica de la seguridad y la responsabilidad jurídica.

Tabla 2.
Matriz analítica de dimensiones de vulnerabilidad de los repositorios digitales de patrimonio cultural

Dimensión	Pregunta que plantea	Expresión en el riesgo	Marcos de referencia
Técnica	¿Es seguro, íntegro y legible el objeto digital a lo largo del tiempo?	Cifrado por ataque, corrupción de bits, obsolescencia de formatos, fallas de interoperabilidad	OAIS (ISO 14721), ISO 16363, PREMIS, NIST CSF
Jurídica	¿Quién responde y bajo qué norma ante la pérdida o el daño?	Vacíos de depósito legal digital, derechos de autor y obras huérfanas, protección de datos	LFDA, Ley General de Archivos, LFPDPPP, LGPDPPSO, RGPD, UNESCO, 2003
Institucional	¿Existen gobernanza, recursos y formación para sostener la custodia?	Ausencia de políticas, presupuesto insuficiente, falta de personal capacitado	Principios CARE, modelos de gobernanza de datos, ética del cuidado

El punto de convergencia que este artículo postula es que ninguna de las tres miradas, por sí sola, basta para gobernar un repositorio: el vacío se localiza precisamente en sus intersecciones.

A partir de esa constatación, se propone un esquema analítico que organiza el resto del artículo. La hipótesis de trabajo es que la ciberseguridad de los repositorios culturales debe entenderse como práctica institucional, y la preservación digital como responsabilidad patrimonial; ambas intuiciones se operacionalizan en una matriz de tres dimensiones de vulnerabilidad, técnica, jurídica e institucional, que se aplica de forma transversal a cada riesgo analizado en las secciones siguientes. La premisa es que ningún riesgo se agota en una sola dimensión: un ataque de *ransomware* es a la vez una falla técnica, un supuesto de responsabilidad jurídica y un problema de gobernanza institucional. La tabla 2 sintetiza este esquema.

Riesgos técnicos de los repositorios digitales de patrimonio cultural

ransomware: cuando el archivo se convierte en rehén

El *ransomware* es, en el panorama actual de amenazas cibernéticas, el riesgo más documentado y de mayor impacto para las instituciones culturales. Se trata de un tipo de *malware* que cifra los archivos del sistema comprometido y exige un rescate (habitualmente en criptomonedas), a cambio de la clave de descifrado. Su relevancia para el patrimonio digital radica en que los archivos culturales e históricos cifrados o destruidos pueden ser irrecuperables en ausencia de respaldos actualizados y correctamente aislados, y en que su valor simbólico hace que las instituciones afectadas se encuentren bajo una presión adicional para ceder ante las exigencias de los atacantes.

Los casos documentados son numerosos y trascienden fronteras. En 2019, City Power, empresa eléctrica municipal de Johannesburgo, reportó un ataque de *ransomware* que afectó sus sistemas y servicios de atención al público (Reuters, 2019). En mayo de 2019, el Gobierno de la Ciudad de Baltimore sufrió un ataque con el *ransomware* RobbinHood que paralizó durante semanas diversos servicios municipales; años después, el Departamento de Justicia de Estados Unidos vinculó ese *malware* con afectaciones de gran escala a servicios públicos locales (Department of Justice, 2025). En 2021, el ataque con REvil al proveedor de servicios tecnológicos Kaseya afectó a organizaciones usuarias de su plataforma VSA, motivo por el cual CISA emitió recomendaciones específicas para proveedores de servicios administrados y sus clientes (Cybersecurity and Infrastructure Security Agency, 2021). En México, un caso ilustrativo de la vulnerabilidad de las grandes instituciones públicas fue la filtración masiva de información de la Secretaría de la Defensa Nacional (SEDENA) en 2022, atribuida al grupo Guacamaya, que expuso documentos institucionales sensibles y evidenció la

relevancia de proteger acervos documentales de valor público (Mexicans Against Corruption and Impunity, 2023; National Security Archive, 2023).

La vulnerabilidad específica de las instituciones culturales ante el *ransomware* responde a varios factores concurrentes. Por un lado, estas instituciones operan con presupuestos ajustados que dejan la ciberseguridad en posiciones subordinadas dentro de las prioridades de gasto. Por otro lado, sus sistemas suelen ser heterogéneos, con software de gestión de colecciones (como DSpace, Omeka, CONTENTdm, Fedora Commons o ICA-AtoM) que en muchas ocasiones se mantiene en versiones desactualizadas por las dificultades de financiamiento y soporte técnico especializado. Finalmente, el personal de estas instituciones (archivistas, bibliotecarios, historiadores, curadores), generalmente no cuenta con formación específica en ciberseguridad, lo que incrementa la exposición a vectores de entrada como el phishing o la descarga de archivos adjuntos maliciosos.

La respuesta ante el *ransomware* no puede limitarse a la instalación de software antivirus. Requiere arquitecturas de respaldo distribuidas y offline (la llamada estrategia 3-2-1: tres copias, en dos medios distintos, una de ellas fuera de línea), planes de continuidad de operaciones, protocolos de segmentación de red que aíslen los sistemas de gestión de colecciones del resto de la infraestructura institucional, y programas de formación continuada del personal en prácticas de higiene digital (NIST, 2024).

Pérdida de integridad documental: la alteración invisible del registro histórico

Más allá de los ataques deliberados, los repositorios digitales enfrentan un riesgo que en ocasiones pasa inadvertido hasta que el daño es irreparable: la pérdida de integridad documental. Esta pérdida puede ocurrir por múltiples causas: degradación de soportes de almacenamiento [*bit rot*], corrupción silenciosa de archivos durante transferencias o migraciones, modificaciones no autorizadas introducidas por fallos de configuración en los sistemas de control de versiones, o alteraciones deliberadas difíciles de detectar si el sistema carece de mecanismos de verificación de integridad.

El *bit rot* (la degradación progresiva de los datos almacenados en medios digitales sin que exista un evento de fallo evidente), es un fenómeno bien documentado en la literatura de preservación digital. Los sistemas de almacenamiento en disco duro convencional exhiben tasas de error no corregibles que, a largo plazo, pueden comprometer la integridad de los datos almacenados (Baker et al., 2006). Los estudios de Lawrence et al. (2000) sobre la preservación de datos científicos y culturales en la Biblioteca del Congreso de Estados Unidos mostraron que un porcentaje significativo

de los archivos digitales almacenados sin verificación periódica presentaban corrupción silenciosa después de cinco años.

Los mecanismos de verificación de integridad más utilizados en el ámbito de la preservación digital son los hashes criptográficos como MD5, SHA-256, SHA-512, entre otros, que generan una huella digital única para cada archivo y permiten detectar cualquier modificación, aunque sea de un solo bit. El modelo OAIS (Open Archival Information System, ISO 14721) establece la verificación periódica de *checksums* como un requisito fundamental para cualquier repositorio que aspire a la preservación a largo plazo. Sin embargo, la implementación efectiva de estos mecanismos en instituciones culturales pequeñas y medianas sigue siendo inconsistente, principalmente por la falta de recursos técnicos y financieros (Lavoie, 2014).

La pérdida de integridad documental tiene consecuencias que van más allá de la preservación técnica: compromete la confiabilidad del registro histórico. Un documento alterado (aunque la alteración sea invisible a la lectura), pierde su carácter de fuente primaria fiable. En el contexto de archivos jurídicos, administrativos o de derechos humanos, donde los documentos digitales pueden constituir evidencia en procesos judiciales o investigaciones históricas, esta dimensión adquiere una gravedad adicional.

Accesos indebidos y filtración de datos: la dimensión de la privacidad en el archivo

Los repositorios digitales de patrimonio cultural no custodian únicamente documentos históricos de acceso libre. Muchos acervos contienen información sensible que, aunque haya sido producida en el pasado, sigue estando protegida por derechos de privacidad o por restricciones de acceso derivadas de compromisos de confidencialidad. Los archivos de salud pública digitalizados pueden contener datos médicos personales; los fondos de correspondencia histórica pueden incluir comunicaciones privadas de personas vivas o de sus descendientes directos; los registros notariales digitalizados pueden exponer información patrimonial o civil; los archivos de organizaciones de derechos humanos pueden contener documentación de víctimas que requiere protección especial.

La Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO, 2025) en México establece obligaciones específicas para las instituciones públicas en el tratamiento de datos personales, incluyendo las que custodian acervos históricos y archivos. Sin embargo, la articulación entre el principio de acceso abierto al patrimonio cultural y la protección de datos personales genera tensiones que el marco normativo no siempre resuelve con suficiente claridad. La excepción de interés

histórico, científico o estadístico prevista en el Reglamento General de Protección de Datos europeo (Reglamento [UE] 2016/679, conocido como RGPD), referencia relevante para el debate latinoamericano, permite la conservación y tratamiento de datos personales con fines de investigación, pero establece garantías específicas que no todos los repositorios implementan de manera consistente.

Los accesos indebidos a repositorios culturales pueden producirse por múltiples vías: credenciales comprometidas, configuraciones incorrectas de los sistemas de control de acceso, vulnerabilidades en las interfaces de usuario de los sistemas de gestión de contenidos, o explotación de APIs mal aseguradas. Las universidades y bibliotecas constituyen blancos frecuentes de este tipo de brechas, dado que concentran grandes volúmenes de datos personales junto con sus acervos. Un ejemplo reciente es la brecha sufrida por Columbia University en 2025, reconocida por la propia institución, que informó que un tercero no autorizado obtuvo información relacionada con admisiones, matrícula, ayuda financiera y ciertos datos personales de empleados (Columbia University Information Technology, 2025). Este tipo de incidentes pone en evidencia que los repositorios digitales no solo custodian patrimonio: también generan y almacenan datos de comportamiento de los usuarios que constituyen, en sí mismos, un activo sensible que requiere protección.

Obsolescencia tecnológica: el riesgo que nadie ve llegar

A diferencia del *ransomware* o las brechas de seguridad, la obsolescencia tecnológica es un riesgo silencioso y de horizonte extendido que, precisamente por eso, suele quedar fuera de las prioridades de gestión institucional. Se manifiesta cuando los formatos de archivo en que se encuentran almacenados los objetos digitales dejan de ser legibles por los sistemas disponibles, o cuando las tecnologías necesarias para interpretar, ejecutar o visualizar esos objetos como software específico, hardware especializado, sistemas operativos descatalogados que dejan de estar disponibles.

La historia de la computación ofrece ejemplos elocuentes de esta problemática. La BBC produjo en 1986, para conmemorar los 900 años del *Domesday Book*, una versión interactiva en videodisco láser que integraba fotografías, mapas, estadísticas y texto de 9 000 escuelas británicas. Para 2002, el proyecto era prácticamente ilegible: el hardware necesario para reproducirlo había dejado de fabricarse y el software de control era incompatible con los sistemas operativos modernos. En contraste, el *Domesday Book* original (el auténtico, en pergamino, del siglo XI) seguía siendo perfectamente legible (Rothenberg, 1999). Este caso, conocido como la "Paradoja del Domesday" o el "Dark Age Digital", ilustra con precisión la paradoja de la preservación

digital: lo que fue creado para durar puede volverse ilegible en décadas, mientras que lo que fue creado en materiales análogos puede sobrevivir siglos.

Los formatos más comúnmente utilizados en proyectos de digitalización de patrimonio cultural, TIFF para imágenes, PDF/A para documentos, WAV para audio, MPEG para vídeo, han sido diseñados específicamente pensando en la preservación a largo plazo, y sus especificaciones son abiertas y documentadas. Sin embargo, muchos repositorios almacenan también objetos en formatos propietarios que dependen de software comercial específico (Adobe Flash, formatos de bases de datos cerrados, aplicaciones interactivas desarrolladas en plataformas descatalogadas, por ejemplo) cuya preservación plantea desafíos mucho más complejos. La emulación consistente en replicar el entorno tecnológico original en un sistema moderno es una de las estrategias de preservación más prometedoras para estos casos, pero su implementación requiere capacidades técnicas especializadas que la mayoría de las instituciones culturales no poseen (Granger, 2000).

Interoperabilidad deficiente: el patrimonio compartimentado

La interoperabilidad, entendida como la capacidad de los sistemas de repositorios para intercambiar, compartir y reutilizar objetos digitales y metadatos de manera coherente, es una condición indispensable para que el patrimonio cultural digital sea genuinamente accesible. Sin interoperabilidad, cada repositorio se convierte en una isla: sus colecciones son consultables desde sus propias interfaces, pero no pueden ser descubiertas ni integradas en búsquedas conjuntas, comparadas con otras colecciones o reutilizadas en proyectos de investigación que requieran datos de múltiples fuentes.

Los principales estándares de interoperabilidad en el ámbito de los repositorios digitales incluyen el protocolo OAI-PMH (Open Archives Initiative Protocol for Metadata Harvesting), que permite la recopilación automatizada de metadatos entre repositorios; el esquema de metadatos Dublin Core, ampliamente adoptado por su simplicidad y compatibilidad; los esquemas más especializados como MARC21, MODS o EAD para bibliotecas y archivos; y los estándares de la Linked Open Data (LOD) que permiten conectar datos de distintos repositorios a través de identificadores permanentes y vocabularios compartidos. En el contexto europeo, Europeana ha impulsado la adopción del Europeana Data Model (EDM) como marco de interoperabilidad para sus más de cincuenta millones de objetos digitales procedentes de instituciones de toda Europa (Isaac y Haslhofer, 2013).

La deficiencia en interoperabilidad no es solo un problema de acceso: es también un riesgo de preservación. Los repositorios que operan con sistemas propietarios o con

implementaciones no estándar de los protocolos de interoperabilidad son más vulnerables a la dependencia tecnológica y a la pérdida de datos en migraciones, porque la extracción y transformación de sus colecciones hacia nuevos sistemas resulta más compleja y propensa a errores. Además, la ausencia de metadatos estandarizados y completos, que frecuentemente acompaña a los proyectos de digitalización desarrollados con recursos insuficientes, dificulta la gestión, el descubrimiento y la preservación a largo plazo de los objetos digitales.

Riesgos legales en los repositorios digitales de patrimonio cultural

Derechos de autor en la digitalización masiva: límites y zonas grises

Uno de los riesgos jurídicos más complejos que enfrentan las instituciones que digitalizan patrimonio cultural es la gestión de los derechos de propiedad intelectual sobre los materiales digitalizados. A primera vista, podría pensarse que los acervos históricos custodiados por bibliotecas nacionales, archivos estatales o museos son de dominio público y, por tanto, libres de restricciones para su digitalización y difusión. La realidad jurídica es considerablemente más complicada.

En México, la Ley Federal del Derecho de Autor establece un plazo de protección de la vida del autor más cien años para la mayoría de las obras. Esto significa que obras del siglo XX (fotografías, grabaciones sonoras, films documentales, manuscritos de escritores o artistas), pueden seguir bajo protección de derechos incluso cuando sus soportes físicos se encuentran en acervos públicos. La digitalización de estos materiales sin la correspondiente gestión de derechos expone a las instituciones a reclamaciones por infracción, aunque operen sin ánimo de lucro y con fines culturales o educativos.

El caso de la Biblioteca Digital de Google Books ilustró globalmente las complejidades de este panorama. El proyecto, que aspiraba a digitalizar millones de libros, se enfrentó a una demanda colectiva de autores y editores que derivó en un proceso judicial de más de una década en Estados Unidos (Authors Guild v. Google). El acuerdo finalmente alcanzado y las disposiciones legales derivadas sentaron precedentes sobre el alcance de las excepciones de uso justo [*fair use*] aplicables a proyectos de digitalización masiva, con consecuencias que se extienden al debate internacional sobre las excepciones educativas y de investigación en el derecho de autor (Band, 2006).

Para las instituciones culturales latinoamericanas, la gestión de derechos en la digitalización presenta desafíos adicionales: la existencia de obras huérfanas u obras cuyos titulares de derechos son desconocidos o imposibles de localizar, para las cuales la Ley Federal del Derecho de Autor mexicana no ofrece una solución jurídica clara que

facilite su digitalización y difusión; la complejidad de las cadenas de titularidad en fotografías, audiovisuales y grabaciones que pueden involucrar múltiples titulares (autores, productores, intérpretes, editoriales); y la frecuente inexistencia de contratos o acuerdos documentados que acrediten las condiciones bajo las cuales ciertos materiales fueron cedidos o donados a las instituciones.

Ausencia de marcos normativos de preservación digital a largo plazo

Más allá de la gestión de derechos, los repositorios digitales de patrimonio cultural operan en un entorno normativo que no ha sido diseñado específicamente para sus necesidades. La Ley General de Archivos de 2018 estableció disposiciones sobre la gestión de documentos electrónicos en el ámbito de los archivos públicos, pero su alcance es fundamentalmente administrativo y no contempla con suficiente especificidad las complejidades de la preservación de objetos culturales digitales como imágenes, audio, vídeo, modelos 3D, bases de datos patrimoniales, publicaciones digitales que requieren estrategias diferenciadas de las aplicables a documentos de texto.

México carece, a la fecha, de una ley específica de depósito legal digital que obligue a los productores de contenido cultural digital tales como editoras, productoras, archivos institucionales a depositar copias de sus producciones en repositorios de preservación nacionales. La Ley Federal sobre Monumentos y Zonas Arqueológicos, Artísticos e Históricos de 1972 protege el patrimonio tangible, pero su extensión al patrimonio digital nacido en entornos digitales es jurídicamente problemática. El Reglamento del Depósito Legal, que obliga a la entrega de publicaciones impresas a la Biblioteca Nacional, no ha sido actualizado para incluir las publicaciones digitales en sus distintas modalidades.

Esta ausencia normativa tiene consecuencias prácticas graves. Sin obligaciones legales claras de preservación, muchas instituciones no desarrollan políticas sistemáticas de gestión del ciclo de vida de los objetos digitales que custodian. Sin marcos de responsabilidad definidos, cuando ocurre una pérdida por ataque cibernético, por fallo técnico o por obsolescencia, no existen mecanismos jurídicos para determinar responsabilidades ni garantizar la restitución del daño. Y sin regulación del depósito legal digital, una parte significativa de la producción cultural digital mexicana contemporánea (publicaciones electrónicas, revistas académicas en línea, audiovisuales independientes o proyectos de arte digital, por mencionar algunas) queda fuera de cualquier sistema de preservación sistemática.

Responsabilidad institucional ante incidentes de seguridad

Cuando un repositorio digital de patrimonio cultural sufre un incidente de seguridad, ya sea un ataque de *ransomware* que destruye colecciones, una filtración de datos que expone información personal de usuarios o de donantes, o una alteración de documentos históricos, la determinación de la responsabilidad jurídica de la institución custodiana es un terreno todavía poco explorado en el derecho mexicano.

Conviene distinguir aquí entre los dos regímenes de protección de datos vigentes en México. La Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP, 2025) rige a las personas físicas y morales del sector privado, mientras que la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO, 2025) rige a los entes públicos. Ambos ordenamientos fueron expedidos mediante decreto publicado en el Diario Oficial de la Federación el 20 de marzo de 2025 y entraron en vigor al día siguiente, abrogando las leyes homónimas de 2010 y 2017 respectivamente. Dado que la mayor parte de los acervos culturales digitales se encuentran bajo custodia de instituciones públicas (bibliotecas nacionales, archivos estatales, universidades públicas), es la LGPDPPSO la que resulta aplicable de manera preponderante. Esta ley establece para las instituciones públicas la obligación de notificar las vulneraciones de seguridad que afecten datos personales y de adoptar medidas técnicas y administrativas para prevenirlas, y su incumplimiento puede derivar en sanciones administrativas. Ahora bien, el panorama institucional se ha modificado de manera relevante: el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), que originalmente recibía dichas notificaciones, fue extinguido tras la reforma constitucional en materia de simplificación orgánica de diciembre de 2024 y la consiguiente legislación secundaria de marzo de 2025, que trasladó sus atribuciones en materia de protección de datos a la Secretaría Anticorrupción y Buen Gobierno, cuyo diseño operativo aún se encontraba en consolidación al momento de redactar este trabajo. Esta reconfiguración genera, al menos transitoriamente, una incertidumbre relevante sobre la autoridad competente y los procedimientos aplicables ante una vulneración. A lo anterior se suma un vacío de fondo: la responsabilidad por pérdida o daño de objetos culturales digitales que no contienen datos personales, pero sí poseen un valor patrimonial y público indiscutible, carece de un tratamiento normativo específico.

La ausencia de seguros especializados para patrimonio digital también contribuye a esta vulnerabilidad institucional. Mientras que el patrimonio tangible, como pinturas, esculturas y documentos históricos materiales, suele estar cubierto por pólizas de seguro de colecciones, el patrimonio digital rara vez cuenta con cobertura aseguradora específica, en parte porque los mecanismos de valoración económica de los objetos

digitales culturales y los procedimientos de peritaje digital en caso de siniestro están todavía en fase de desarrollo (UNESCO, 2020).

La tabla 3 sintetiza los principales riesgos identificados, categorizados por su naturaleza (técnica o legal), el nivel de impacto estimado y las medidas de mitigación más relevantes disponibles en la literatura especializada.

Tabla 3
Síntesis de riesgos técnicos y legales en repositorios digitales de patrimonio cultural

Riesgo	Naturaleza	Impacto potencial	Medida de mitigación principal
Ransomware	Técnica	Alto / Pérdida total	Estrategia 3-2-1 de respaldo; segmentación de red; formación del personal
Pérdida de integridad documental	Técnica	Alto / Daño silencioso	Verificación periódica de checksums (SHA-256); modelo OAIS
Accesos indebidos / filtración	Técnica-Legal	Medio-Alto / Exposición de datos	Control de acceso por roles; cifrado de datos sensibles; auditorías regulares
Obsolescencia tecnológica	Técnica	Alto / Inaccesibilidad futura	Uso de formatos abiertos (TIFF, PDF/A, WAV); estrategias de emulación y migración
Interoperabilidad deficiente	Técnica-Institucional	Medio / Aislamiento del acervo	Implementación de OAI-PMH; metadatos Dublin Core o EDM; LOD
Conflictos de derechos de autor	Legal	Medio-Alto / Reclamaciones legales	Revisión jurídica previa a digitalización; gestión de obras

			huérfanas; licencias Creative Commons
Vacíos en depósito legal digital	Legal	Alto / Pérdida del registro cultural	Reforma normativa; políticas institucionales de depósito voluntario
Ausencia de responsabilidad normativa	Legal-Institucional	Medio / Falta de rendición de cuentas ante incidentes	Políticas de seguridad documentadas; cumplimiento LGPDPPSO; notificación a la autoridad competente.
Nota: elaboración propia a partir de la revisión de literatura especializada.			

Resultados y discusión

El análisis desarrollado a lo largo del artículo permite consolidar un conjunto de resultados que trascienden la mera catalogación de riesgos para proponer una lectura integrada del problema y sus implicaciones para la política institucional y la investigación en humanidades digitales.

La confirmación de que la vulnerabilidad de los repositorios digitales de patrimonio cultural no puede explicarse desde una perspectiva unidimensional. Los riesgos técnicos y los riesgos legales no son fenómenos independientes que puedan atenderse por separado: están profundamente imbricados. Un ataque de *ransomware*, por ejemplo, no es solo un problema de infraestructura informática; es también un problema de responsabilidad jurídica, de cobertura aseguradora, de protección de datos y, en el plano más profundo, de gobernanza institucional. Del mismo modo, un vacío normativo en materia de depósito legal digital no es solo un problema de política legislativa: tiene consecuencias técnicas directas, porque sin obligaciones normativas que lo impulsen, las instituciones carecen de incentivos para desarrollar las capacidades técnicas de preservación a largo plazo.

Este hallazgo conecta con los planteamientos de Brügger (2018) sobre la fragilidad del patrimonio digital nacido en entornos en red, donde la preservación depende de decisiones técnicas, institucionales y normativas que se toman (o se omiten) simultáneamente en múltiples niveles. La ausencia de coordinación entre estos niveles, que en el contexto mexicano es particularmente visible en la distancia entre las disposiciones de la Ley General de Archivos, las políticas de acceso abierto de las universidades y los requerimientos técnicos de los estándares de preservación

internacionales, genera un espacio de vulnerabilidad estructural que ninguna medida técnica aislada puede subsanar.

Las instituciones culturales de menor tamaño como archivos municipales, bibliotecas comunitarias, acervos de organizaciones civiles, museos de sitio, son desproporcionadamente vulnerables frente a las instituciones grandes que cuentan con recursos técnicos y humanos especializados. Esta asimetría no solo implica una distribución inequitativa del riesgo: implica también una distribución inequitativa de la pérdida. Son precisamente los acervos de las comunidades con menor poder institucional, como los archivos de comunidades indígenas que documentan su historia y lengua, los fondos fotográficos de organizaciones de derechos humanos o los registros de movimientos sociales locales, los que se encuentran en mayor riesgo de perderse, porque sus custodios suelen contar con menos recursos para implementar medidas técnicas, jurídicas e institucionales de protección.

Esta desigualdad en la vulnerabilidad tiene una dimensión ética y política que las humanidades digitales no pueden ignorar. Warwick, Terras y Nyhan (2012) han señalado que los proyectos de humanidades digitales tienden a reproducir las asimetrías de poder existentes en el campo académico: las instituciones mejor financiadas concentran los proyectos de mayor visibilidad y los recursos técnicos más sofisticados, mientras que los acervos de menor visibilidad institucional permanecen en la sombra de la digitalización. Extender esta crítica al ámbito de la preservación digital implica reconocer que las políticas de ciberseguridad y de gestión del riesgo también tienen una dimensión de justicia patrimonial.

La formación especializada como el recurso más escaso y estratégico en el ecosistema de los repositorios culturales. Tanto la literatura especializada en ciberseguridad institucional (NIST, 2024; National Research Council, 2015) como los estudios sobre preservación digital (Lavoie, 2014; National Research Council, 2015) coinciden en señalar que el factor humano es el vector de entrada más frecuente en los incidentes de seguridad y la causa más común de los errores de preservación. El personal de los repositorios culturales (archivistas, bibliotecarios, curadores y gestores de colecciones) generalmente no cuenta con formación específica en ciberseguridad, en gestión de riesgos digitales ni en los estándares técnicos de preservación digital.

Esta brecha formativa no puede resolverse con cursos ocasionales de sensibilización: requiere la incorporación de contenidos de ciberseguridad y preservación digital en los currículos de los programas de formación universitaria en archivística, bibliotecología, gestión del patrimonio cultural y humanidades digitales, así como el desarrollo de

programas de formación continua para profesionales en activo. En México, algunas instituciones como el Centro Universitario de Investigaciones Bibliotecológicas (CUIB) de la UNAM y la Escuela Nacional de Biblioteconomía y Archivonomía (ENBA) han iniciado la incorporación de contenidos de humanidades digitales en sus programas, pero la dimensión de la ciberseguridad aplicada a los repositorios culturales sigue siendo marginal en los planes de estudios disponibles.

En términos de discusión con la literatura preexistente, el presente artículo dialoga con y amplía tres líneas de trabajo relevantes. La primera es la literatura sobre preservación digital, que ha producido marcos conceptuales y estándares técnicos de gran valor (ISO 14721:2012, OAIS; ISO 16363:2012, para la auditoría de repositorios de confianza), pero que con frecuencia aborda la ciberseguridad como un tema marginal o la integra de manera incompleta en sus modelos (Lavoie, 2014; Thibodeau, 2002). La segunda es la literatura de ciberseguridad institucional, que ha desarrollado marcos robustos de gestión del riesgo (NIST, 2024; ISO/IEC 27001:2022) pero que generalmente no contempla las especificidades del patrimonio cultural (la irreversibilidad de la pérdida, el valor simbólico de los objetos, la dimensión pública del deber de custodia) como factores diferenciadores en el análisis de riesgos. La tercera es la literatura de humanidades digitales, que ha teorizado sobre la ética del cuidado de los datos digitales (Flanders y Jannidis, 2019; Drucker, 2021) pero que ha tendido a subvalorar la dimensión técnica de la seguridad y los aspectos normativos de la responsabilidad jurídica.

El aporte central de este artículo reside en proponer la intersección de estas tres líneas como el espacio conceptual y práctico donde deben situarse las políticas de gestión de repositorios digitales de patrimonio cultural. Esta intersección no es un ejercicio meramente académico: tiene consecuencias directas para la manera en que las instituciones diseñan sus sistemas, forman a su personal, negocian sus marcos normativos y asumen sus responsabilidades ante la sociedad.

Conclusiones

Este artículo se propuso responder qué riesgos técnicos y legales comprometen la preservación y el acceso sostenible del patrimonio cultural alojado en repositorios digitales, y qué condiciones institucionales se requieren para mitigarlos en el contexto mexicano y latinoamericano. El recorrido permite ofrecer una respuesta articulada en torno a las tres preguntas secundarias planteadas: las dimensiones técnica, jurídica e institucional se imbrican en cada riesgo y no pueden atenderse de forma aislada; el ordenamiento mexicano presenta vacíos relevantes, agravados por la reciente

reconfiguración institucional en materia de protección de datos; y las humanidades digitales están en posición de articular los lenguajes técnico, jurídico y patrimonial que la respuesta exige.

El patrimonio cultural en sus formas digitales enfrenta hoy amenazas que no son ficticias ni especulativas: son reales, documentadas y en algunos casos han producido pérdidas de difícil o imposible reparación. El *ransomware* ha secuestrado colecciones institucionales completas. La degradación silenciosa de bits ha corrompido archivos que nadie verificaba. La obsolescencia tecnológica ha vuelto ilegibles objetos digitales producidos hace apenas dos décadas. Los vacíos normativos han dejado sin protección a categorías enteras de producción cultural digital que, sencillamente, no estaban previstas cuando se redactaron las leyes vigentes. Ante este panorama, ni el voluntarismo institucional ni la inversión aislada en soluciones técnicas son respuestas suficientes.

Lo que este artículo argumenta es que la preservación sostenible del patrimonio cultural digital requiere una transformación en la manera en que concebimos la responsabilidad institucional sobre los objetos digitales. Esa transformación implica, cuando menos, cuatro orientaciones de política que las instituciones custodias deben asumir de manera articulada. A manera de corolario se menciona a la adopción de modelos de gobernanza digital que integren ciberseguridad, preservación y gestión de derechos como funciones institucionales de igual rango que las de adquisición, descripción y difusión de colecciones. Así como a la implementación sistemática de estándares de preservación reconocidos internacionalmente (OAIS/ISO 14721, formatos abiertos, verificación periódica de integridad), como prácticas no opcionales sino constitutivas de la gestión profesional de repositorios.

Resulta imperante al contexto mencionar que la orientación es la demanda y la incidencia activa en la construcción de marcos normativos más completos, que incluyan: una legislación de depósito legal digital con alcance nacional; disposiciones específicas sobre responsabilidad institucional ante incidentes de seguridad que afecten patrimonio cultural; y soluciones jurídicas para la digitalización y difusión de obras huérfanas que equilibren la protección de derechos con el acceso al patrimonio. Así pues, es necesario impulsar a la formación del talento humano especializado que pueda sostener estas transformaciones: archivistas con competencias digitales, bibliotecarios con comprensión de la ciberseguridad, humanistas digitales con sensibilidad jurídica y juristas con conocimiento de las especificidades del patrimonio cultural digital.

Las humanidades digitales tienen una responsabilidad específica en este proceso. Como campo que se sitúa en la intersección entre el conocimiento humanístico y los métodos digitales, están en posición privilegiada para articular los distintos lenguajes, técnico, jurídico, archivístico, humanístico, que la preservación del patrimonio cultural digital requiere. Esta articulación no es un lujo intelectual: es una necesidad práctica urgente, porque el patrimonio que se pierda hoy no podrá recuperarse mañana.

Como líneas de trabajo futuro, este artículo sugiere tres prioridades de investigación:

1. El levantamiento sistemático del estado de implementación de políticas de ciberseguridad y preservación digital en los repositorios culturales mexicanos, mediante estudios de campo que permitan caracterizar la brecha entre las prácticas recomendadas por los estándares internacionales y las capacidades institucionales reales.
2. El desarrollo de marcos conceptuales y metodológicos específicos para la valoración del riesgo en repositorios de patrimonio cultural, que incorporen la dimensión del valor simbólico e histórico de los objetos como una variable que los marcos de ciberseguridad empresarial no contemplan de manera adecuada.
3. La articulación de propuestas de reforma normativa concretas, elaboradas en colaboración entre juristas, tecnólogos de la información y especialistas en patrimonio cultural, que permitan dotar al sistema jurídico mexicano de las herramientas necesarias para proteger el patrimonio cultural digital con la misma profundidad con que protege el patrimonio tangible.

Obras citadas

Baker, M., Shah, M., Rosenthal, D. S. H., Roussopoulos, M., Maniatis, P., Giuli, T. J., y Bungale, P. (2006). A fresh look at the reliability of long-term digital storage. *Proceedings of the 1st ACM SIGOPS/EuroSys European Conference on Computer Systems*, 221-234. https://doi.org/10.1145/1217935.1217957

Band, J. (2006). *The Google Library Project: The copyright debate*. American Library Association. https://alair.ala.org/items/6a6a2d34-3e28-4904-9eb1-53ded4100d44

Besek, J. M., LeFurgy, W. G., Rasenberger, M., Weston, C. D., Muir, A., Atkinson, B., Carroll, E., Coates, J., Fitzgerald, B. F., y Mossink, W. (2008). *International study on the impact of copyright law on digital preservation*. Library of Congress. https://www.digitalpreservation.gov/documents/digital_preservation_final_report2008.pdf

Brügger, N. (2018). *The archived web: Doing history in the digital age*. MIT Press.

Burdick, A., Drucker, J., Lunenfeld, P., Presner, T., y Schnapp, J. (2012). *Digital_Humanities*. MIT Press.

Carroll, S. R., Garba, I., Figueroa-Rodríguez, O. L., Holbrook, J., Lovett, R., Materechera, S., Parsons, M., Raseroka, K., Rodriguez-Lonebear, D., Rowe, R., Sara, R., Walker, J. D., Anderson, J., y Hudson, M. (2020). The CARE principles for Indigenous data governance. *Data Science Journal, 19*(1), Article 43. https://doi.org/10.5334/dsj-2020-043

Columbia University Information Technology. (2025, August 5). *Updating our community on the cyber incident*. Columbia University. https://www.cuit.columbia.edu/content/updating-our-community-cyber-incident

Cybersecurity and Infrastructure Security Agency. (2021, July 4). *CISA-FBI guidance for MSPs and their customers affected by the Kaseya VSA supply-chain ransomware attack*. https://www.cisa.gov/news-events/alerts/2021/07/04/cisa-fbi-guidance-msps-and-their-customers-affected-kaseya-vsa-supply-chain-ransomware-attack

Department of Justice. (2025, May 27). *Iranian man pleaded guilty to role in RobbinHood ransomware*. Office of Public Affairs. https://www.justice.gov/opa/pr/iranian-man-pleaded-guilty-role-robbinhood-ransomware

Directiva (UE) 2019/790 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, sobre los derechos de autor y derechos afines en el mercado único digital. (2019). *Diario Oficial de la Unión Europea, L 130*, 92-125. https://eur-lex.europa.eu/eli/dir/2019/790/oj

Drucker, J. (2021). *The digital humanities coursebook: An introduction to digital methods for research and scholarship*. Routledge.

Flanders, J., y Jannidis, F. (Eds.). (2019). *The shape of data in the digital humanities: Modeling texts and text-based resources*. Routledge.

Granger, S. (2000). Emulation as a digital preservation strategy. *D-Lib Magazine, 6*(10). https://www.dlib.org/dlib/october00/granger/10granger.html

International Organization for Standardization [ISO]. (2012a). *Space data and information transfer systems - Open archival information system (OAIS) - Reference model (ISO 14721:2012)*. ISO.

International Organization for Standardization [ISO]. (2012b). *Space data and information transfer systems - Audit and certification of trustworthy digital repositories (ISO 16363:2012)*. ISO.

International Organization for Standardization & International Electrotechnical Commission [ISO/IEC]. (2022). *Information security, cybersecurity and privacy protection - Information security management systems - Requirements (ISO/IEC 27001:2022)*. ISO.

Isaac, A., y Haslhofer, B. (2013). Europeana Linked Open Data - data.europeana.eu. *Semantic Web, 4*(3), 291-297. https://doi.org/10.3233/SW-120092

Lavoie, B. (2014). *The Open Archival Information System (OAIS) reference model: Introductory guide* (2nd ed.). Digital Preservation Coalition. https://doi.org/10.7207/twr14-02

Lawrence, G. W., Kehoe, W. R., Rieger, O. Y., Walters, W. H., y Kenney, A. R. (2000). *Risk management of digital information: A file format investigation*. Council on Library and Information Resources. https://www.clir.org/pubs/reports/pub93/

Ley Federal de Protección de Datos Personales en Posesión de los Particulares [LFPDPPP]. (2025, 20 de marzo). *Diario Oficial de la Federación*. https://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf

Ley Federal del Derecho de Autor. (1996, 24 de diciembre). *Diario Oficial de la Federación*. Última reforma publicada el 1 de julio de 2020. https://www.diputados.gob.mx/LeyesBiblio/pdf/LFDA.pdf

Ley General de Archivos. (2018, 15 de junio). *Diario Oficial de la Federación*. https://www.diputados.gob.mx/LeyesBiblio/pdf/LGA.pdf

Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados [LGPDPPSO]. (2025, 20 de marzo). *Diario Oficial de la Federación*. https://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf

Lynch, C. (1999). Canonicalization: A fundamental tool to facilitate preservation and management of digital information. *D-Lib Magazine, 5*(9). https://www.dlib.org/dlib/september99/09lynch.html

Mexicans Against Corruption and Impunity. (2023, February 20). *Hackeo histórico a servidores de la SEDENA*. https://contralacorrupcion.mx/anuario-de-la-corrupcion-2022/hackeo-historico-a-servidores-de-la-sedena

National Institute of Standards and Technology [NIST]. (2024). *The NIST Cybersecurity Framework (CSF) 2.0* (NIST CSWP 29). U.S. Department of Commerce. https://doi.org/10.6028/NIST.CSWP.29

National Research Council. (2015). *Preparing the workforce for digital curation*. The National Academies Press. https://doi.org/10.17226/18590

National Security Archive. (2023, March 10). *Guacamaya leaks and the Ayotzinapa case*. The George Washington University. https://nsarchive.gwu.edu/briefing-book/mexico-ayotzinapa/2023-03-10/guacamaya-leaks-and-ayotzinapa-case

PREMIS Editorial Committee. (2015). *PREMIS data dictionary for preservation metadata* (Version 3.0). Library of Congress. https://www.loc.gov/standards/premis/v3/

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos [RGPD]. (2016). *Diario Oficial de la Unión Europea, L 119*, 1-88.

Reuters. (2019, July 25). *Johannesburg power body hit by ransomware attack*. https://www.reuters.com/article/world/johannesburg-power-body-hit-by-ransomware-attack-idUSKCN1UK15G/

Rid, T., y McBurney, P. (2012). Cyber-weapons. *The RUSI Journal, 157*(1), 6-13. https://doi.org/10.1080/03071847.2012.664354

Rinehart, A. K., Prud'homme, P. A., y Huot, A. R. (2014). Overwhelmed to action: Digital preservation challenges at the under-resourced institution. *OCLC Systems & Services: International Digital Library Perspectives, 30*(1), 28-42. https://doi.org/10.1108/OCLC-06-2013-0019

Rothenberg, J. (1999). *Avoiding technological quicksand: Finding a viable technical foundation for digital preservation*. Council on Library and Information Resources. https://www.clir.org/pubs/reports/rothenberg/

Terras, M., Nyhan, J., y Vanhoutte, E. (Eds.). (2016). *Defining digital humanities: A reader*. Ashgate Publishing.

Thibodeau, K. (2002). Overview of technological approaches to digital preservation and challenges in coming years. En *The state of digital preservation: An international perspective* (pp. 4-31). Council on Library and Information Resources.

UNESCO. (2003). *Carta sobre la preservación del patrimonio digital*. https://unesdoc.unesco.org/ark:/48223/pf0000179529_spa

UNESCO. (2020). *Managing risks at UNESCO World Heritage properties: A practical guide*. UNESCO World Heritage Centre. https://whc.unesco.org/en/managing-risk

Warwick, C., Terras, M., y Nyhan, J. (Eds.). (2012). *Digital humanities in practice*. Facet Publishing.