REVISTA CIENTÍFICA

Vol. 22, No.2 (2026) mayo-agosto, ISSN electrónico: 1683-8947

bibliotecas anales de investigación

BIBLIOTECA NACIONAL DE CUBA JOSÉ MARTÍ

REPOSITORIOS DIGITALES UNIVERSITARIOS: MARCOS DE EVALUACIÓN E INTEGRACIÓN DE LOS PRINCIPIOS TRUST, ZERO TRUST Y FAIR

UNIVERSITY DIGITAL REPOSITORIES: FRAMEWORKS FOR EVALUATING AND INTEGRATING TRUST, ZERO TRUST, AND FAIR PRINCIPLES

Sánchez-Rivera, María Teresa
Universidad Técnica de Manabí, Ecuador
maría.sanchez@utm.edu.ec
https://orcid.org.//0000-0001-7894-5969

Martínez-Rodríguez, Ailín
Universidad de La Habana, Cuba
ailin@fcom.uh.cu
https://orcid.org/0000-0003-1969-9176

Rivera, Zoia
Universidad de La Habana, Cuba
zoia@fcom.uh.cu
https://orcid.org/0000-0002-7017- 5493

Santovenia-Diaz, Javier Ramón
Centro Politécnico Fernando Aguado y Rico, La Habana, Cuba
interactivo@infomed.sld.cu
https://orcid.org/0000-0002-4169-3371

Rivero-Torres, Carlos Eduardo
Universidad Técnica de Manabí, Ecuador
carlos.rivero@utm.edu.ec
https://orcid.org/0000-0003-1956-7448

autor de correspondencia: maría.sanchez@utm.edu.ec

Recibido: 27 de noviembre 2025
Revisado: 11 febrero de 2026
Aprobado: 9 de abril de 2026

Cómo citar: Sánchez-Rivera, M. T; Martínez-Rodríguez, A; Rivera, Z; Santovenia-Diaz, J. R; Rivero-Torres, C. E. (2026). Repositorios digitales universitarios: marcos de evaluación e integración de los principios TRUST, Zero Trust y FAIR. *Bibliotecas. Anales de Investigacion;22*(2), 1-11

RESUMEN

Los repositorios digitales universitarios (RDU) se han consolidado como infraestructura crítica para la ciencia abierta, al articular preservación, visibilidad e interoperabilidad de la producción académica. Sin embargo, su madurez operativa no se limita a la disponibilidad de la tecnología: requiere un marco de evaluación que integre políticas, calidad de los metadatos, integridad de los metadatos, experiencia del usuario y, especialmente, confianza y seguridad. El artículo presenta una revisión de la literatura y un análisis comparativo de métodos y herramientas para la evaluación y certificación de repositorios (p. 2). Por ejemplo. DINI, RECOLECTA-FECYT, OpenAIRE, COAR, CoreTrustSeal e ISO 16363 y ofrece una matriz de métricas integrada para repositorios universitarios. El principal aporte es la convergencia de tres enfoques complementarios: (i) CONFIANZA como principio de confiabilidad y sostenibilidad; (ii) la "confianza cero" como modelo de ciberseguridad basado en la verificación continua y el mínimo privilegio; y (iii) FAIR como criterio para mejorar la localización, accesibilidad, interoperabilidad y reutilización de objetos digitales. Los resultados sintetizan aspectos prácticos y métricas y proporcionan una tabla comparativa que vincula TRUST-Zero Trust-FAIRNESS con medidas de gestión, protección y seguridad. Se concluye que la adopción coordinada de estos principios incrementa la transparencia, resiliencia, calidad de metadatos, cumplimiento normativo y posicionamiento del repositorio en ecosistemas de recolección y descubrimiento, fortaleciendo su rol estratégico en universidades.
PALABRAS CLAVE: repositorios institucionales; repositorios universitarios; evaluación; ciencia abierta; TRUST; Zero Trust; FAIR; interoperabilidad; preservación digital.

ABSTRACT

University digital repositories (UDRs) have become critical infrastructure for open science by enabling long-term preservation, visibility and interoperability of scholarly outputs. Yet repository maturity goes beyond technical deployment: it requires assessment frameworks that combine policy, metadata quality, preservation, user experience, and crucially trust and security. This paper undertakes a documentary review and comparative analysis of leading repository assessment instruments (e.g., DINI, RECOLECTA-FECYT, OpenAIRE, COAR, CoreTrustSeal and ISO 16363), and proposes an integrated indicator matrix tailored to university repositories. The main contribution is an operational convergence of three complementary approaches: (i) TRUST as principles for repository transparency, responsibility, user focus, sustainability and technology; (ii) Zero Trust as a cybersecurity paradigm grounded in continuous verification and least privilege; and (iii) FAIR as guiding principles to enhance findability, accessibility, interoperability and reuse of digital objects. Results synthesize actionable dimensions, criteria and indicators and provide a comparative table linking TRUST–Zero Trust–FAIR to governance, preservation and security practices.
KEYWORDS: institutional repositories; university repositories; assessment; open science; TRUST; Zero Trust; FAIR; interoperability; digital preservation.

INTRODUCCIÓN

Los repositorios digitales universitarios (RDU) también denominados repositorios institucionales son plataformas destinadas a reunir, preservar y difundir la producción académica de una institución (artículos, tesis, datos, objetos de aprendizaje, entre otros). Su relevancia se refuerza en el marco de la ciencia abierta: promueven acceso oportuno, trazabilidad del conocimiento y visibilidad de la investigación, así como la preservación a largo plazo de activos digitales (UNESCO, 2021).

En el ecosistema contemporáneo, "existir en la web" no es equivalente a "ser visible". La inclusión en directorios y agregadores depende de criterios de calidad editorial, exposición de metadatos e interoperabilidad, por ejemplo, OpenDOAR establece criterios de inclusión claros que requieren requisitos de información, políticas organizativas y acceso efectivo al contenido (OpenDOAR, s.f.). Además, directrices como OpenAIRE estandarizan los perfiles de metadatos y las referencias de identificadores persistentes para facilitar la recopilación y el enriquecimiento semántico (OpenAIRE, 2023). Este contexto crea un doble problema. En primer lugar, la evaluación: coexisten múltiples directrices y modelos (p. ej. DINI, RECOLECTA-FECYT, sistemas de auditoría) con criterios parcialmente superpuestos, lo que dificulta

alcanzar diagnósticos comparables y planes de mejora unificados. En segundo lugar, confianza y seguridad: los repositorios gestionan activos digitales y metadatos, lo que tiene consecuencias legales y de reputación; Por lo tanto, la gobernanza debe integrar principios de confianza (CONFIANZA) y una arquitectura de seguridad moderna (Confianza Cero) sin comprometer la interoperabilidad y la reutilización (FAIR). Este artículo tiene tres objetivos: (a) distinguir conceptualmente el repositorio universitario de su tipología; b) comparar métodos de evaluación y normas/certificaciones relevantes; y (c) proponer una matriz de indicadores integrada que integre TRUST, Zero Trust y FAIR como un trío para mejorar la calidad, seguridad y reutilización de los objetos digitales. Esta contribución es aplicable: traducir documentos y estándares en criterios de desempeño útiles para la autoevaluación, la planificación estratégica y la preparación para procesos de auditoría o certificación.

METODOLOGÍA

Se adoptó un enfoque cualitativo de revisión documental con análisis de contenido, orientado a identificar dimensiones, criterios e indicadores de evaluación de repositorios digitales universitarios. Se consideraron documentos normativos, guías técnicas y literatura académica de acceso público. Entre los instrumentos y estándares incluidos figuran: DINI Certificate 2019, Guía RECOLECTA-FECYT (4.ª edición), OpenAIRE Guidelines (v4), recomendaciones COAR sobre repositorios de nueva generación, CoreTrustSeal Requirements 2023–2025, así como estándares de preservación y auditoría (OAIS y ISO 16363). Los criterios de selección incluyen fuentes que: a) presenten criterios/indicadores claros de evaluación o certificación; (b) abordar cuestiones de cumplimiento, conducta y/o seguridad/confianza; (c) es aplicable a publicaciones universitarias, repositorios de datos u objetos digitales. Priorice las fuentes con DOI o URL estables. Se construye una matriz de extracción con los siguientes campos: dimensiones, criterios, indicadores, evidencia y nivel de implementación. Luego se realizó una codificación temática para agrupar los indicadores en dimensiones macro: (1) gobernanza y políticas; (2) recaudación y gestión; (3) metadatos e interoperabilidad; (4) protección; (5) servicio y experiencia del usuario; (6) métricas/visibilidad; y (7) seguridad y gestión de riesgos. Finalmente, en el mapa de actividades se incluyeron los principios TRUST (Lin et al., 2020), Zero Trust (Rose et al., 2020) y FAIR (Wilkinson et al., 2016; RDA FAIR Data Maturity Model Working Group, 2020).

Salida metodológica. El resultado es una propuesta de indicadores observables, con evidencias verificables, diseñada para apoyar autoevaluaciones, planes de mejora y auditorías internas. La matriz se concibe como base para validaciones posteriores (p. ej., aplicación en una muestra regional de repositorios universitarios y análisis de brechas).

RESULTADOS

Delimitación conceptual: repositorios y bases de datos

Aunque en el discurso institucional a veces se confunden, una base de datos y un repositorio cumplen funciones distintas. La base de datos se orienta al almacenamiento y consulta estructurada de registros (con énfasis en recuperación y administración), mientras que el repositorio integra curación, preservación, visibilidad, exposición de metadatos e interoperabilidad para la difusión y reutilización de objetos digitales.

Tabla 1

Diferencias funcionales entre base de datos y repositorio digital universitario

Aspecto	Base de datos	Repositorio digital universitario
Propósito principal	Almacenar y permitir consultas estructuradas sobre registros.	Preservar y difundir objetos digitales y metadatos, habilitando reutilización.
Objeto gestionado	Registros y campos; puede no incluir el objeto digital completo.	Objetos digitales + metadatos ricos + relaciones (p. ej., proyecto, financiación, autoría).
Interoperabilidad	Depende del diseño; no siempre expone metadatos a recolectores externos.	Integra protocolos/perfiles (p. ej., OAI-PMH, directrices OpenAIRE) para recolección e indexación.
Ciclo de vida y preservación	Respaldo y mantenimiento orientados a continuidad operativa.	Curación, control de versiones, fijación e integridad, planes OAIS de preservación.

Nota. Elaboración propia a partir de recomendaciones de repositorios y preservación (COAR, 2017; OpenDOAR, s. f.; CCSDS, 2024).

Tipología de repositorios universitarios

Los repositorios pueden diferenciarse por la naturaleza de sus objetos, su comunidad objetivo y el régimen de gestión. En entornos universitarios, la tipología se vincula con el portafolio institucional: publicaciones académicas, datos de investigación, materiales docentes, patrimonio cultural o documentación administrativa seleccionada. La Tabla 2 sintetiza las tipologías más frecuentes.

Tabla 2

Tipos de repositorios y contenidos característicos en el ámbito universitario

Tipo	Descripción operativa	Contenidos típicos
Repositorio institutional	Reúne y preserva la producción académica de una universidad con políticas de depósito y licenciamiento.	Artículos, tesis, informes, libros, ponencias, preprints.
Repositorio de datos	Gestiona datasets y materiales asociados con curación, preservación y (si aplica) embargos/control de acceso.	Datos, código, documentación, plan de gestión de datos
Repositorio temático	Se especializa en disciplina; es el hogar de muchas organizaciones y comunidades de práctica.	Literatura y/o datos de un dominio científico.
Repositorio editorial	La atención se centra en las publicaciones que llevan el sello de prensa universitaria y en su conservación.	Libros, capítulos, revistas, manuales, guías.
Repositorio de objetos de aprendizaje	Apoyar recursos educativos reutilizables utilizando metadatos pedagógicos.	OER, videos, guías didácticas, simulaciones, evaluaciones.
Repositorio patrimonial	Preserva patrimonio cultural digitalizado con descripción archivística/museológica.	Fondos, colecciones especiales, imágenes, audio, piezas museográficas.
Repositorio governmental/administrativo	Gestiona documentación institucional con controles estrictos de acceso y trazabilidad.	Normativa interna, memorias, documentación administrativa seleccionada.
Repositorio de investigación	Prioriza outputs de investigación y su trazabilidad (PID, proyectos, financiación).	Artículos, datasets vinculados, informes técnicos, productos de proyectos.

Nota. Elaboración propia a partir de recomendaciones para repositorios y ciencia abierta (UNESCO, 2021; COAR, 2017; OpenAIRE, 2023).

Síntesis comparada de metodologías y estándares de evaluación

El análisis documental evidencia una evolución desde enfoques centrados en volumen de contenido hacia modelos multidimensionales que integran: calidad de metadatos e interoperabilidad, políticas y aspectos legales, servicios y experiencia de usuario, preservación y sostenibilidad, y más recientemente confianza, auditoría y seguridad. La Tabla 3 resume instrumentos representativos y el foco de sus criterios.

Tabla 3
Instrumentos y enfoques de evaluación/certificación de repositorios institucionales

Referencias	Propósito	Dimensiones/Criterios (síntesis)	Ejemplo de indicadores observables
Kim & Kim (2008)	Validar indicadores para un consorcio de repositorios universitarios.	Marco de categorías con validación empírica en dCollection.	Cobertura de colección; accesibilidad; uso; políticas.
Cassella (2010)	Proponer indicadores de desempeño para medir éxito e impacto.	Indicadores internos/externos (perspectiva tipo balanced scorecard).	Crecimiento del depósito; texto completo; cooperación; financiación.
Barrionuevo (2010)	Definir indicadores de calidad para repositorios institucionales.	Calidad, servicios de valor añadido, visibilidad e impacto.	Cumplimiento OA; exposición OAI-PMH; estadísticas; servicios.
Fushimi et al. (2011)	Aplicar indicadores a repositorios universitarios (teoría a práctica).	Colección; servicios; metadatos; interfaz; recursos.	Metadatos mínimos; políticas; navegación; soporte.
Serrano-Vicente et al. (2014)	Establecer indicadores de evaluación para repositorios OA.	Tecnología, procedimientos, contenidos, marketing y personal.	Licencias; interoperabilidad; difusión; recursos humanos.
DINI (2019)	Certificar servicios de publicación OA con requisitos mínimos.	Criterios: visibilidad, políticas, metadatos, interfaces, métricas, preservación.	OAI-PMH conforme; info legal; estadísticas; disponibilidad.
RECOLECTA-FECYT (2021)	Guía de autoevaluación para repositorios de investigación.	Visibilidad, políticas, aspectos legales, metadatos, interoperabilidad, estadísticas y preservación.	Política de depósito; licencias; OAI-PMH; calidad de registros.
OpenAIRE (2023)	Alinear repositorios con requisitos de agregación e interoperabilidad.	Directrices de metadatos y exposición para recolección.	Perfiles; vocabularios; PID (ORCID/DOI); enlaces a financiación.
Core Trust Seal (2022)	Certificar repositorios de datos confiables.	Gestión organizacional, curación, preservación, infraestructura.	Plan de preservación; integridad; continuidad; documentación.
ISO 16363:2025 / CCSDS	Auditar y certificar repositorios digitales confiables.	Métricas para infraestructura organizacional, gestión de objetos seguridad/infraestructura.	Gestión de riesgos; controles; evidencia OAIS; auditoría.

Nota. Síntesis basada en las fuentes citadas en las referencias.

Integración de TRUST, Zero Trust y FAIR

Los marcos revisados convergen en tres necesidades: confiabilidad institucional (gobernanza y sostenibilidad), seguridad frente a amenazas contemporáneas y máxima reutilización de objetos digitales. En este trabajo se integran TRUST, Zero Trust y FAIR como capas complementarias: TRUST orienta la confiabilidad del servicio (transparencia, responsabilidad, foco en usuarios, sostenibilidad y tecnología); Zero Trust aporta control de acceso y mitigación de riesgos centrado en verificación continua; y FAIR operacionaliza calidad y reutilización mediante identificadores persistentes, metadatos ricos y estándares interoperables.

Tabla 4

Mapeo operativo de TRUST, Zero Trust y FAIR en funciones del repositorio

Función/Dominio	TRUST (foco)	Zero Trust (control)	FAIR (criterio)	Evidencias/indicadores recomendados
Gobernanza y transparencia	Transparencia; Responsabilidad	Políticas de identidad/acceso explícitas	R1: licenciamiento y procedencia	Políticas públicas; roles; trazabilidad; licencias claras.
Identidades y acceso	Foco en usuarios	Verificación continua; mínimo privilegio; MFA	A1/A2: accesibilidad con protocolos apropiados	MFA; control por roles; auditoría; gestión de embargos.
Metadatos e interoperabilidad	Tecnología	Validación/seguridad de APIs y servicios	F1–F4; I1–I3	OAI-PMH; perfiles OpenAIRE; PID; vocabularios controlados.
Curación y calidad	Responsabilidad	Cadena de custodia en ingesta y edición	R1.2/R1.3	Revisión de metadatos; checksums; control de versiones; documentación.
Preservación digital	Sostenibilidad; Tecnología	Resiliencia/continuidad	R: reutilización a largo plazo	OAIS; planes de preservación; copias geográficas; pruebas de restauración.
Métricas y rendición de cuentas	Transparencia	Monitoreo y detección de anomalías	F: descubrimiento	Estadísticas; dashboards; alertas; registro de cambios.
Riesgos y seguridad	Sostenibilidad	Microsegmentación; respuesta a incidentes	A: acceso controlado cuando aplica	Modelo de amenazas; cifrado; hardening; incident response.

Nota. Elaboración propia a partir de Lin et al. (2020), Rose et al. (2020), Wilkinson et al. (2016) y RDA FAIR Data Maturity Model Working Group (2020).

Tabla comparativa de principios y aportes a repositorios digitales

Para facilitar decisiones de implementación, se comparan el alcance conceptual y los aportes diferenciales de cada enfoque. En conjunto, la tríada TRUST–Zero Trust–FAIR fortalece repositorios universitarios en tres frentes: confiabilidad institucional, resiliencia y seguridad, y reutilización /interoperabilidad.

Tabla 5

Comparación de TRUST, Zero Trust y FAIR y su aporte a repositorios digitales universitarios

Enfoque	Objetivo	Principios /Componentes	¿Qué mejora en el repositorio?	Riesgo que mitigan	Indicadores prácticos
TRUST	Confiabilidad y sostenibilidad del repositorio.	Transparencia; Responsabilidad; Usuario; Sostenibilidad; Tecnología.	Políticas claras, continuidad del servicio, curación documentada.	Opacidad, pérdida de confianza, fallas de preservación	Políticas públicas; RACI; plan de preservación; evidencia de curación.
Zero Trust	Reducir superficie de ataque y controlar accesos.	Verificar explícitamente; mínimo privilegio; asumir brecha; segmentación; monitoreo.	Control granular, auditoría y trazabilidad de acciones críticas.	Acceso indebido, manipulación, abuso de credenciales.	MFA; RBAC/ABAC; logs; microsegmentación; respuesta a incidentes.
FAIR	Maximizar localización, accesibilidad, interoperabilidad y reutilización.	F A I R + indicadores de madurez.	Visibilidad, recolección por agregadores, citabilidad y reutilización.	Silos de información; baja recuperación; imposibilidad de reutilización.	PID; metadatos ricos; vocabularios; estándares; licencias claras.

Nota. Elaboración propia con base en Lin et al. (2020), Rose et al. (2020), Wilkinson et al. (2016), CoreTrustSeal (2022) y RDA (2020).

Matriz integradora de indicadores para autoevaluación de repositorios universitarios

A partir de la codificación temática y la comparación de instrumentos, se propone una matriz integradora con indicadores observables. La Tabla 6 organiza criterios mínimos por dimensión, sugiere evidencias verificables y vincula el criterio con TRUST, Zero Trust y/o FAIR cuando corresponde. Esta matriz puede adaptarse como lista de verificación para auditorías internas o para planes de mejora anual.

Tabla 6

Matriz integradora de indicadores y evidencias verificables

Dimensión	Criterio	Indicador sugerido	Evidencia verificable	Principio asociado
Gobernanza	Política de depósito y alcance	Política pública y vigente; define tipos de objetos, embargos y responsabilidades.	Documento publicado en el repositorio/sitio institucional; fecha de revisión.	TRUST (T,R,S)
Gobernanza	Licencias y Reutilización	Licencias explícitas por ítem (p. ej., CC) y términos de uso del sitio.	Metadatos con licencia; página de términos; coherencia con política.	FAIR (R1)
Metadatos	Identificadores persistentes	Uso sistemático de PID (Handle/DOI) y ORCID para autoría cuando aplica.	Registro de PID; validación de enlaces; tasa de completitud.	FAIR (F1), OpenAIRE
Interoperabilidad	Exposición y	OAI-PMH habilitado;	Endpoint OAI-	FAIR (F4/I)

	conformidad	cumplimiento de perfiles (p. ej., OpenAIRE v4).	PMH público; validaciones; reportes de agregadores.	
Preservación	Integridad y fijación	Checksums por archivo; verificación periódica; bit-preservation.	Logs de fijación; reportes de verificación; procedimientos.	TRUST (T,S)
Seguridad	Autenticación robusta	MFA para administración; control por roles y auditoría de cambios.	Configuración MFA; matriz RBAC; bitácoras inmutables.	Zero Trust
Servicios	Experiencia de usuario	Guías de depósito y uso; accesibilidad; soporte y contacto.	Manual público; canales de soporte; tiempos de respuesta.	TRUST (U)
Métricas	Estadísticas y transparencia	Métricas de uso y depósito; dashboards; reportes periódicos.	Panel de estadísticas; informes; metodología de conteo.	TRUST (T)

Nota. La matriz integra criterios recurrentes en DINI (2019), RECOLECTA-FECYT (2021), OpenAIRE (2023), CoreTrustSeal (2022), ISO 16363 (2025) y NIST SP 800-207 (Rose et al., 2020).

DISCUSIÓN

El resultado más consistente del análisis comparado es la comprensión del repositorio como sistema socio-técnico. Las herramientas de evaluación tienden a combinar requisitos tecnológicos con procesos, roles y evidencias documentales. En otras palabras, un repositorio "maduro" no se define por su software, sino por su capacidad de sostener políticas, curación, preservación y seguridad en el tiempo.

TRUST y los esquemas de certificación (CoreTrustSeal e ISO 16363) desplazan el foco hacia la trazabilidad: no basta declarar políticas; debe demostrarse su aplicación mediante documentación, registros y prácticas estables.

En los repositorios universitarios, es necesario establecer deberes institucionales (responsable del servicio, curación, seguridad, apoyo), procedimientos (ingreso, revisión de metadatos, conservación, eliminación/retención) y supervisión (integridad, continuidad, auditoría) .

Zero Trust, que fue concebido originalmente para estructuras empresariales, es relevante debido a la desaparición del "perímetro" convencional .En repositorios, la amenaza no solo proviene del exterior: incluye credenciales comprometidas, cargas dañinas, uso inadecuado de APIs, manipulación social y cambios no autorizados en metadatos .La implementación gradual de Zero Trust podría comenzar con la autenticación multifactor, control basado en roles, segmentación de componentes y supervisión continua de acciones privilegiadas .

FAIR añade una dimensión de reutilización que complementa la confianza y seguridad .Un repositorio puede ser seguro y sostenible, pero si no proporciona metadatos detallados, identificadores persistentes y vocabularios controlados, su valor científico se ve afectado: se volverá inaccesible e incompatible con servicios externos .Por lo tanto, la intersección de TRUST, Zero Trust y FAIR elimina la falsa dicotomía entre apertura y seguridad: una apertura responsable requiere tanto gobernanza como controles de acceso y métodos de conservación .

Consecuencias para la gestión. La matriz integradora facilita la priorización de mejoras basadas en su impacto .Algunas acciones que ofrecen alta relación coste-beneficio incluyen: a) verificar perfiles OpenAIRE y calidad de OAI-PMH; b) estandarizar licencias por ítem; c) fortalecer PID (Handle/DOI/ORCID) y enlaces a financiamiento/proyectos; d) aplicar sumas de verificación y rutinas de control; e) habilitar autenticación

multifactor para gestión y auditoría de cambios; y f) publicar informes de métricas y políticas para aumentar la transparencia y la rendición de cuentas .

CONCLUSIONES

Los repositorios digitales universitarios son infraestructura crítica para la ciencia abierta; su desempeño debe evaluarse más allá de la disponibilidad tecnológica, incorporando gobernanza, preservación, interoperabilidad, experiencia de usuario, métricas y seguridad.

La comparación de instrumentos (DINI, RECOLECTA-FECYT, OpenAIRE, COAR, Core TrustSeal e ISO 16363) evidencia convergencia hacia modelos basados en evidencia documental y control de riesgos, orientados a fortalecer confiabilidad y sostenibilidad del servicio.

La combinación de TRUST, Zero Trust y FAIR crea una operativa en tres partes: TRUST promueve la claridad y el desarrollo sostenible; Zero Trust minimiza las amenazas de acceso y alteraciones inapropiadas; y FAIR mejora la calidad de los metadatos, la interoperabilidad y la citación, ayudando a integrar el repositorio en entornos de descubrimiento.

La tabla sugerida (Tabla 6) puede ser utilizada como una lista de verificación para autoevaluarse y como fundamento para estrategias de mejora continua

Como agenda futura, se recomienda validar empíricamente la matriz en una muestra regional de repositorios universitarios, y evaluar su consistencia mediante revisión por expertos y análisis de concordancia entre evaluadores.

Limitaciones y líneas futuras

Este trabajo se basa en revisión documental y, por tanto, no reporta resultados de aplicación en un conjunto específico de repositorios. La propuesta de matriz requiere validación contextual (tipo de repositorio, disciplina, marco legal nacional, capacidad tecnológica y recursos humanos).

En investigaciones futuras se sugiere: (a) aplicar la matriz a repositorios universitarios de una región (por ejemplo, un país o provincia) para estimar niveles de cumplimiento; (b) desarrollar ponderaciones por dimensión (según misión institucional); (c) incorporar métricas FAIR automáticas (por ejemplo, herramientas de evaluación de madurez) y (d) explorar indicadores de impacto científico y social asociados al repositorio.

REFERENCIAS BIBLIOGRÁFICAS

Barrionuevo Almuzara, L. (2010). Indicadores de calidad para evaluar repositorios institucionales. *Rebiun*. http://hdl.handle.net/20.500.11967/789

Barrueco Cruz, J. M., et al. (2021). *Guía para la evaluación de repositorios institucionales de investigación (4.ª ed.). FECYT–REBIUN–RECOLECTA*. https://www.fecyt.es/system/files/2024-08/2021guiaevaluacionrecolecta.pdf

Cassella, M. (2010). Institutional repositories: An internal and external perspective on the value of IRs for researchers' communities. *LIBER Quarterly, 20*(2), 210–225. https://doi.org/10.18352/lq.7980

Confederation of Open Access Repositories (COAR) Next Generation Repositories Working Group. (2017). Next generation repositories: Behaviours and technical recommendations. *Zenodo*. https://doi.org/10.5281/zenodo.8077381

Consultative Committee for Space Data Systems (CCSDS). (2024). *Audit and certification of trustworthy digital repositories (CCSDS 652.0-M-2, Issue 2)*. https://ccsds.org/Pubs/652x0m2.pdf

Consultative Committee for Space Data Systems (CCSDS). (2024). *Reference model for an Open Archival Information System (OAIS) (CCSDS 650.0-M-3, Issue 3)*. https://ccsds.org/Pubs/650x0m3.pdf

CoreTrustSeal Standards and Certification Board. (2022). CoreTrustSeal Requirements 2023–2025 (Version 01.00). *Zenodo*. https://doi.org/10.5281/zenodo.7051012

De Giusti, M. R. (2021). Calidad en los repositorios digitales: Los principios TRUST para repositorios de datos. *Revista Iberoamericana de Tecnología en Educación y Educación en Tecnología*, (29), 55–59. https://doi.org/10.24215/18509959.29.e6

Devaraju, A., Mokrane, M., Cepinskas, L., Huber, R., Herterich, P., de Vries, J., & Davidson, J. (2021). From conceptualization to implementation: FAIR assessment of research data objects. *Data Science Journal, 20*, 4. https://doi.org/10.5334/dsj-2021-004

DINI. (2019). *DINI Certificate for Open Access Publication Services 2019*. Humboldt-Universität zu Berlin. https://edoc.hu-berlin.de/bitstreams/49ac5903-7801-484c-97f7-31bab69e8608/download

Fernández-Ramos, A. (2021). Value-added services in institutional repositories in Spanish public universities. *Information Research, 26*(1), paper 895. https://informationr.net/ir/26-1/paper895.html

Fushimi, M. S., Pené, M. G., Unzurrunzaga, C., & Genovés, P. (2011). Indicadores para evaluar repositorios universitarios argentinos: De la teoría a la práctica. *Memoria Académica*. https://www.memoria.fahce.unlp.edu.ar/trab_eventos/ev.878/ev.878.pdf

ISO. (2025). ISO 16363:2025—Audit and certification of trustworthy digital repositories. International Organization for Standardization. https://www.iso.org/standard/87472.html

Kim, Y. H., & Kim, H. H. (2008). Development and validation of evaluation indicators for a consortium of institutional repositories: A case study of dCollection. *Journal of the American Society for Information Science and Technology, 59*(8), 1282–1294. https://doi.org/10.1002/asi.20818

Lin, D., Crabtree, J., Dillo, I., Downs, R. R., Edmunds, R., Giaretta, D., De Giusti, M., L'Hours, H., Hugo, W., Jenkyns, R., Khodiyar, V., Martone, M. E., Mokrane, M., Navale, V., Petters, J., Sierman, B., Sokolova, D., Stockhause, M., Yarmey, L., & Zarnitz, M. (2020). *The TRUST Principles for digital repositories. Scientific Data*, 7, 144. https://doi.org/10.1038/s41597-020-0486-7

OpenAIRE. (2023). *OpenAIRE Guidelines for Literature Repository Managers* (v4). https://guidelines.openaire.eu/en/latest/literature/index.html

OpenDOAR. (s. f.). *Inclusion criteria*. https://opendoar.ac.uk/help/inclusion-criteria

Poveda, E. B. (2022). *Estándares, auditoría, madurez y planificación estratégica en repositorios digitales.* https://www.redalyc.org/journal/1790/179072459005/179072459005.pdf

Research Data Alliance (RDA) *FAIR Data Maturity Model Working Group. (2020). FAIR Data Maturity Model: Specification and guidelines. Research Data Alliance*. https://doi.org/10.15497/RDA00050

Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). *Zero Trust Architecture (NIST Special Publication 800-207). National Institute of Standards and Technology*. https://doi.org/10.6028/NIST.SP.800-207

Sanabria, J. S. G. (2023). Evaluación de repositorios institucionales: una aproximación desde las experiencias latinoamericanas. *ACOFI Papers*. https://acofipapers.org/index.php/eiei/article/download/2991/2193/7911

Serrano-Vicente, R., Melero, R., & Abadal, E. (2014). Indicadores para la evaluación de repositorios institucionales de acceso abierto. *Anales de Documentación, 17*(2). https://doi.org/10.6018/analesdoc.17.2.190821

UNESCO. (2021). *UNESCO Recommendation on Open Science.* https://unesdoc.unesco.org/ark:/48223/pf0000379949

Wilkinson, M. D., Dumontier, M., Aalbersberg, I. J., Appleton, G., Axton, M., Baak, A., Blomberg, N., Boiten, J.-W., da Silva Santos, L. B., Bourne, P. E., Bouwman, J., Brookes, A. J., Clark, T., Crosas, M., Dillo, I., Dumon, O., Edmunds, S., Evelo, C. T., Finkers, R., … Mons, B. (2016). *The FAIR Guiding Principles for scientific data management and stewardship. Scientific Data*, 3, 160018. https://doi.org/10.1038/sdata.2016.18

Yeo, P. P., & Choh, N. L. (2023). *Evaluating an institutional repository: A case study of a university in Singapore.* Singapore Management University. https://ink.library.smu.edu.sg/cgi/viewcontent.cgi?article=1220&context=library_research