Volumen 5 | Número 12 | Octubre-diciembre - 2025 | ISSN: 2959-9040 | ISNN-L: 2959-9040 | Pág. 589 - 599 https://revistaimpulso.org/

Más allá del directorio: replanteando el active directory como eje estratégico ***de planificación tecnológica en el sector público peruano***

Beyond the directory: rethinking active directory as a strategic axis of technological planning in the peruvian public sector

Para além do diretório: repensando o Active Directory como eixo estratégico de planejamento tecnológico no setor público peruano

Tania Adalid Mori Becerril
tamoribec@ucvvirtual.edu.pe
https://orcid.org/0009-0008-0572-9964
Universidad César Vallejo. Lima, Perú

Maritza Elizabeth Zamora Centurión
mzamorac@ucvvirtual.edu.pe
https://orcid.org/0009-0007-4799-9615
Universidad César Vallejo. Lima, Perú

Hernán Cervantes Lino Gamarra
hernanlinog@ucvvirtual.edu.pe
https://orcid.org/0000-0003-4410-5253
Universidad César Vallejo. Lima, Perú

Eduardo Humberto Poletti Gaitan
epolettig@ucvvirtual.edu.pe
https://orcid.org/0000-0002-2143-4444
Universidad César Vallejo. Lima, Perú

Luis Arnaldo Godoy Fuentes
lgodoyf@ucvvirtual.edu.pe
https://orcid.org/0000-0002-3910-219X
Universidad César Vallejo. Lima, Perú

Jonathan Alexis Puente Zamora
jpuentez@ucvvirtual.edu.pe
https://orcid.org/0000-0001-6109-4416
Universidad César Vallejo. Lima, Perú

http://doi.org/10.59659/impulso.v.5i12.205

Artículo recibido 4 de agosto 2025 | Aceptado 26 de septiembre 2025 | Publicado 3 de octubre 2025

RESUMEN

El estudio analiza el Active Directory como eje estratégico de la planificación tecnológica en el sector público peruano. Su objetivo fue evaluar su impacto en la gestión de recursos tecnológicos a partir de tres dimensiones: planificación, acceso y administración, y control y monitoreo. La investigación empleó un diseño aplicado basado en revisión estructurada y observación directa, utilizando muestreo probabilístico estratificado. La recolección de datos se realizó mediante fichaje de registro validado por expertos, lo que garantizó uniformidad y claridad en el procesamiento de la información. Los resultados evidencian que el Active Directory, cuando se implementa estratégicamente, transforma la gestión tecnológica institucional, elevando la planificación de una actividad documental a un proceso ejecutable, optimizando la administración de accesos como ventaja estratégica y fortaleciendo el control y monitoreo mediante capacidades proactivas. Se concluye que el Active Directory debe entenderse como infraestructura tecnológica esencial, cuya incorporación genera mejoras cuantificables en eficiencia, seguridad estructural y gobernanza medible.

Palabras clave: Active Directory; Planificación tecnológica; Sector público; Gestión de recursos; Gobernanza digital

ABSTRACT

The study analyzes Active Directory as a strategic axis of technological planning in the Peruvian public sector. Its objective was to evaluate its impact on technological resource management across three dimensions: planning, access and administration, and control and monitoring. The research employed an applied design based on structured review and direct observation, using stratified probabilistic sampling. Data collection was conducted through expert-validated record indexing, ensuring uniformity and clarity in information processing. The results show that Active Directory, when strategically implemented, transforms institutional technological management by elevating planning from a documentary activity to an executable process, optimizing access administration as a strategic advantage, and strengthening control and monitoring through proactive capabilities. It is concluded that Active Directory should be understood as essential technological infrastructure, whose incorporation generates quantifiable improvements in efficiency, structural security, and measurable governance.

Keywords: Active Directory; Technological planning; Public sector; Resource management; Digital governance

RESUMO

O estudo analisa o Active Directory como eixo estratégico do planejamento tecnológico no setor público peruano. Seu objetivo foi avaliar seu impacto na gestão de recursos tecnológicos a partir de três dimensões: planejamento, acesso e administração, e controle e monitoramento. A pesquisa utilizou um delineamento aplicado baseado em revisão estruturada e observação direta, com amostragem probabilística estratificada. A coleta de dados foi realizada por meio de fichamento de registro validado por especialistas, garantindo uniformidade e clareza no processamento das informações. Os resultados mostram que o Active Directory, quando implementado estrategicamente, transforma a gestão tecnológica institucional ao elevar o planejamento de uma atividade documental para um processo executável, otimizar a administração de acessos como vantagem estratégica e fortalecer o controle e o monitoramento por meio de capacidades proativas. Conclui-se que o Active Directory deve ser compreendido como infraestrutura tecnológica essencial, cuja adoção gera melhorias quantificáveis em eficiência, segurança estrutural e governança mensurável.

Palavras-chave: Active Directory; Planejamento tecnológico; Setor público; Gestão de recursos; Governança digital

INTRODUCCIÓN

En la actualidad, la transformación digital en el sector público constituye un factor estratégico para garantizar eficiencia, seguridad y continuidad operativa en la gestión institucional. La creciente dependencia de sistemas informáticos y plataformas digitales ha resaltado la necesidad de contar con infraestructuras que centralicen la administración de identidades, permisos y recursos tecnológicos. En este marco, el Active Directory emerge como un componente crítico que no solo facilita la autenticación y el control de accesos, sino que se convierte en un eje integrador de la gobernanza tecnológica, la ciberseguridad y la planificación estratégica en las organizaciones estatales.

Particularmente en el Perú, donde la modernización digital avanza de manera desigual y está tensionada por fragmentaciones históricas en la gestión tecnológica, el Active Directory representa una oportunidad para consolidar procesos, reducir duplicidades y fortalecer la resiliencia institucional frente a amenazas cibernéticas. Su implementación centralizada permite articular políticas de acceso, trazabilidad de usuarios y protección de la información, convirtiéndose en un instrumento capaz de alinear la infraestructura

tecnológica con los objetivos de desarrollo institucional y los lineamientos de la Agenda 2030, especialmente en lo relacionado con innovación, infraestructura y sostenibilidad digital.

En este contexto, la finalidad del presente estudio consistió en esclarecer cómo el Active Directory, en su condición de orquestador y maestro de la identidad digital, así como cimiento de la agilidad operativa, genera seguridad virtual perimetral dinámica y fortalece la gobernanza tecnológica en el sector público. La Agenda 2030, particularmente el ODS 9, vinculado a Industrias, Innovación e Infraestructura, impulsa la renovación tecnológica en la gestión interna de las organizaciones (Montero, 2021).

En el Perú, la transformación digital del Estado ha avanzado de manera desigual, tensionada entre mandatos normativos de modernización administrativa y limitaciones estructurales derivadas de la fragmentación tecnológica acumulada por décadas de gestión sectorial. En este contexto, el Active Directory, concebido originalmente como una herramienta técnica para la administración de identidades y recursos, se presenta como un componente crítico para repensar la planificación tecnológica estatal. Su función trasciende la autenticación de usuarios o control de accesos, convirtiéndose en una infraestructura estratégica de soberanía digital capaz de articular interoperabilidad, ciberseguridad y gobernanza de datos en todos los niveles del aparato público.

A pesar de su implementación masiva en ministerios y gobiernos regionales, el AD ha operado de manera dispersa, sin un enfoque de arquitectura unificada que permita integrarlo plenamente a los objetivos de desarrollo institucional. De allí surge el interés académico y técnico por analizar su dimensión operativa, consolidándose como eje articulador de la planificación tecnológica gubernamental dentro de la agenda de Gobierno Digital (Diksha et al., 2023). Entre los elementos críticos se encuentra la contextualización de accesos, que habilita controles de seguridad basados en el quién, el dónde, el cuándo y el cómo se accede, sentando las bases para un modelo de confianza cero (Zero Trust) y estableciendo un centro de operaciones de crisis digital con estrategias de hardening, detección de amenazas y recuperación ante desastres.

Esta relevancia justifica la inversión en modernización y diseño estratégico del AD, no como un gasto operativo, sino como una inversión esencial para blindar el presente y futuro digital de las instituciones (Camavilca, 2025). La implementación estandarizada y con compliance garantiza un entorno controlado, eficiente y alineado con las políticas corporativas, superando la histórica fragmentación de la gestión tecnológica en el sector público peruano.

Como directorio jerárquico centralizado, el AD puede ser el núcleo estructural de una gestión integrada de servicios tecnológicos, siempre que su adopción se vincule a la planificación institucional de mediano y largo plazo. Sin embargo, los marcos de gobernanza digital vigentes, como el Decreto Supremo 029-2021-PCM o la Política Nacional de Transformación Digital 2030, han abordado de manera marginal

el rol estratégico de los directorios activos, dejando vacíos en la integración de seguridad, planeamiento, gestión documental y administración de servicios.

A nivel internacional, organismos como el Canadian Centre for Cyber Security (2023) destacan que la gestión centralizada de directorios es clave para la estrategia organizacional, articulando políticas de acceso, monitoreo, auditoría y resiliencia tecnológica. En México, el Centro de Auditoría Superior de la Federación (2021) identificó debilidades en más del 47 % de las dependencias federales por ausencia de soluciones de directorio activo, lo que generaba falta de trazabilidad y gestión ineficaz de permisos. En Perú, la administración manual de cuentas y recursos tecnológicos conlleva retrasos y consumo excesivo de horas hombre, afectando procesos institucionales (INEI, 2022; Centro Nacional de Seguridad Digital, 2022).

La literatura reciente evidencia un cambio de paradigma: el AD deja de ser un servicio meramente técnico para convertirse en un ecosistema vivo que articula eficiencia operativa, gobernanza de datos y resiliencia ante ciberataques. Estudios de vanguardia destacan la aplicación de grafos de ataque, algoritmos de inteligencia artificial y optimización evolutiva para la defensa proactiva del AD (Guo et al., 2021; Diksha et al., 2023; Huy et al., 2024; Ngo et al., 2024). Estas estrategias permiten identificar rutas de ataque, optimizar la detección temprana mediante señuelos y mejorar la resiliencia institucional frente a amenazas complejas, acercando la teoría a prácticas defensivas aplicables en entornos críticos del sector público.

Desde la perspectiva de gestión, el marco de ITIL v4 y la Teoría General de Sistemas (Ronquillo et al., 2024; Axelos, 2019) permiten conceptualizar al AD como un subsistema tecnológico que, al centralizar planificación, acceso y control, genera impactos positivos y sinérgicos en la eficiencia organizacional. La conceptualización tripartita de Cordero y Ramón (2021) —planificación de recursos, administración de acceso y monitoreo— permite evaluar de manera estructurada la eficacia del AD, reforzada por evidencia empírica en estudios de eficiencia operativa y seguridad (Ocrospoma y Romero, 2021; Hernández et al., 2021; Echeverri, 2024).

En síntesis, la introducción del presente estudio establece al Active Directory como un instrumento estratégico y multidimensional en el sector público, cuya correcta implementación permite articular gobernanza tecnológica, seguridad, eficiencia operativa y resiliencia digital. Su estudio no solo aborda vacíos prácticos en la gestión de identidades y recursos, sino que también conecta la evidencia teórica con la aplicación concreta en entornos gubernamentales, brindando una base sólida para la investigación, planteando objetivos claros y justificando su relevancia dentro de la modernización tecnológica del Estado peruano (Montero, 2021; Diksha et al., 2023; Camavilca, 2025).

MÉTODO

La investigación fue de tipo aplicada, caracterizada por utilizar conocimientos científicos para identificar problemas concretos en situaciones determinadas (Osada y Salvador, 2021), utilizando técnicas

estadísticas para obtener data con la finalidad de reflejar la postulación a este instrumento (Acosta et al., 2021).El diseño fue de revisión (Hadi et al., 2023) y observación directa de los efectos de la intervención bajo un muestreo probabilístico estratificado (Romero et al., 2021), la técnica de recolección de datos fue el fichaje (Vásquez et al., 2023) como una técnica documental que permite el registro explícito, ordenado y clasificado de información relevante, la cual, de acuerdo con Álvarez et al. (2021), funciona como una herramienta que posibilita estructurar y ordenar información crucial, asegurando uniformidad y claridad. La metodología se estructuró para proporcionar una comprensión rigurosa, transparente y replicable del proceso investigativo, fundamentando cada decisión técnica y conceptual.

El estudio se orientó bajo un enfoque aplicado, dado que buscó examinar un problema concreto de la administración pública peruana y generar evidencia empírica útil para la toma de decisiones institucionales. Esta elección responde a la necesidad de vincular el análisis del Active Directory con la operatividad real de la gestión tecnológica, permitiendo evaluar su impacto directo sobre procesos y recursos.

En correspondencia con dicho enfoque, se adoptó un diseño metodológico de revisión estructurada y observación directa, cuyo propósito fue articular el análisis teórico con evidencia procedente de la práctica institucional. La revisión estructurada permitió delimitar el estado del conocimiento, mientras que la observación directa facilitó evaluar los efectos operativos derivados de la intervención tecnológica. Este diseño se justifica debido a la naturaleza híbrida del fenómeno estudiado: una plataforma técnica cuyo impacto se manifiesta tanto en la arquitectura organizacional como en los flujos de trabajo cotidianos.

La población de estudio estuvo comprendida por los recursos tecnológicos y usuarios institucionales involucrados en los procesos de planificación, administración de accesos y control operativo. Para garantizar la representatividad se aplicó un muestreo probabilístico estratificado, el cual distribuyó proporcionalmente los elementos muestrales según áreas funcionales, asegurando así la validez en la comparación entre dimensiones analizadas.

La recolección de datos se efectuó mediante la técnica de fichaje documental, seleccionada por su capacidad de registrar información de manera ordenada, explícita y replicable. Los instrumentos de fichaje fueron sometidos a validación por expertos, lo que aseguró claridad operacional, coherencia conceptual y uniformidad en la sistematización de datos. Este procedimiento fue necesario para evitar sesgos interpretativos en el tratamiento de indicadores relacionados con cumplimiento de planificación, cobertura de accesos y tiempos de atención de requerimientos.

En conjunto, la metodología se diseñó para capturar con fidelidad los efectos del Active Directory sobre la gestión de recursos tecnológicos, garantizando una línea de análisis objetiva, estructurada y alineada con los objetivos de la investigación.

RESULTADOS Y DISCUSIÓN

Los resultados de esta investigación permiten articular una discusión que trasciende la mera constatación empírica para proponer un proceso de subsunción conceptual: el Active Directory, desde la categoría de herramienta técnica, emerge de los datos como un elemento que debe ser subsumido en una categoría superior: la de eje estratégico para la planificación tecnológica en el sector público.

La mejora más dramática se registró en la dimensión de Los resultados planificación, donde el cumplimiento de actividades tecnológicas pasó de 24.91% a 94.81%. Este salto cuantitativo no representa simplemente un incremento de productividad; constituye la materialización de una capacidad de gobierno sobre los recursos tecnológicos que antes era inexistente. Este hallazgo subsume la noción de planificación tecnológica, definida por Ocrospoma y Romero (2021) como la definición anticipada de políticas y asignación de infraestructura, bajo el paraguas de una plataforma centralizada que la hace ejecutable y medible.

En la dimensión de acceso y administración, la evolución del 29.84% al 98.91% de usuarios con acceso activo no solo resuelve un problema operativo de gestión de identidades, sino que redefine el perímetro de seguridad institucional. Este resultado valida empíricamente el postulado del CCN-CERT (2023) que señala la gestión deficiente de usuarios como la principal causa de brechas de seguridad. La implementación del AD subsume la gestión de accesos, antes fragmentada y vulnerable, en un modelo de seguridad centralizada y auditada.

La dimensión de control y monitoreo ofrece quizás la métrica más elocuente de la transformación operativa: la reducción del tiempo de atención de requerimientos de 44.76 a 18.07 minutos (59.6%). Esta mejora no se explica por una simple aceleración de procesos manuales, sino por la subsunción de tareas operativas repetitivas en procesos automatizados. Lo que INEI (2022) identificaba como la pérdida del 45% del tiempo de TI en tareas repetitivas, es precisamente lo que el AD logra erradicar.

Finalmente, esta discusión conduce a una subsunción teórica que integra los hallazgos. La Teoría General de Sistemas (Ronquillo et al., 2024) encuentra en estos resultados una validación práctica: el AD actúa como el elemento de interconexión y control que armoniza los subsistemas (usuarios, equipos, políticas) que antes operaban de forma caótica, elevando el desempeño del sistema organizacional en su conjunto. Simultáneamente, el marco ITIL v4 (Axelos, 2019) ve materializado su principio de gestión estratégica de recursos a través de una plataforma concreta que permite planificar, entregar y monitorear servicios de TI de manera alineada con los objetivos del negocio.

Desde una mirada de gobernanza y política pública, el replanteamiento del Active Directory implica reconfigurar las relaciones entre infraestructura tecnológica, arquitectura institucional y legitimidad administrativa. En un Estado descentralizado como el peruano, la planificación tecnológica no puede

entenderse como una mera función informática, sino como un instrumento de coordinación multinivel que articule a los gobiernos locales y regionales con las directrices nacionales.

La implementación de Active Directory Federations en la nube pública podría permitir dicha unificación bajo esquemas de autenticación única, con control centralizado, auditoría continua y políticas de acceso basadas en roles. No obstante, el desafío no es únicamente técnico: requiere un rediseño de procesos, competencias y estructuras institucionales que trasciendan la dependencia del área de sistemas, integrando a las direcciones de planificación, presupuesto y recursos humanos (Yuhang y He, 2023).

En el plano de la seguridad y soberanía tecnológica, el Active Directory implica políticas integradas de defensa y monitoreo continuo, articuladas a los planes nacionales de ciberseguridad y gestión de riesgos digitales. En el contexto peruano, donde la cultura de ciberseguridad aún es incipiente, las medidas suelen centrarse en la protección perimetral, sin considerar la gestión de identidades como la primera línea de defensa. Ello exige una planificación estratégica que incorpore el modelo de resiliencia tecnológica del Estado, vinculado al Sistema Nacional de Planeamiento Estratégico, de modo que la seguridad no sea un fin aislado, sino una dimensión transversal de la gestión pública digital.

Discusión

El análisis de los resultados evidencia una transformación sustantiva en la gestión tecnológica institucional, la cual adquiere sentido pleno cuando se interpreta a la luz de los marcos teóricos y del contexto del sector público peruano. La magnitud de los cambios observados confirma que el Active Directory trasciende su concepción tradicional como herramienta administrativa, integrándose como un componente estructural para la planificación tecnológica, la seguridad digital y la gobernanza organizacional.

Desde la perspectiva de la Teoría General de Sistemas, la centralización generada por el Active Directory repara una falla histórica del aparato público: la fragmentación de identidades, recursos, permisos y procesos. Los resultados muestran que, al consolidar estos subsistemas, se incrementa la coherencia interna y se reduce la entropía organizacional, lo que se refleja en mejoras cuantificables en planificación, seguridad y control operativo. Este hallazgo confirma que la intervención tecnológica produce un reordenamiento sistémico y no únicamente operativo.

Asimismo, el estudio corrobora los postulados de ITIL v4, que plantea la gestión estratégica de recursos como pilar para la entrega eficiente de servicios. La evidencia demuestra que la planificación tecnológica deja de ser un ejercicio documental y se convierte en un proceso ejecutable, auditado y medible, lo cual constituye un cambio de paradigma respecto a la práctica habitual en el sector público peruano. En esa línea, el incremento del 24.91% al 94.81% en la ejecución de actividades de planificación no es solo un indicador técnico, sino una manifestación del fortalecimiento de la gobernanza institucional.

En relación con la seguridad digital, los resultados validan lo señalado por organismos internacionales, que identifican la mala gestión de identidades como causa principal de brechas de seguridad. La cobertura del 98.91% en administración de accesos confirma que el Active Directory opera como un sólido perímetro lógico de control, mitigando riesgos estructurales y consolidando un modelo de seguridad basado en la centralización y la trazabilidad.

Finalmente, se reconocen las limitaciones del estudio, entre ellas la dependencia del contexto institucional específico y la falta de integración con modelos predictivos avanzados, como los propuestos en el estado del arte mediante grafos de ataque e inteligencia artificial. También se identifica como limitación la necesidad de intervenciones organizacionales complementarias en capacitación y rediseño de procesos para maximizar los beneficios del sistema.

En conjunto, la discusión revela que el Active Directory se erige como un eje articulador en la planificación tecnológica pública, ofreciendo evidencia empírica de una transformación sistémica, medible y sostenible, a la vez que abre nuevas líneas de investigación relacionadas con interoperabilidad, automatización avanzada y resiliencia digital en el sector gubernamental.

CONCLUSIONES

El presente estudio evidencia que la implementación del Active Directory en el sector público peruano tiene un impacto significativo en la eficiencia operativa, la seguridad informática y la gobernanza institucional. Los hallazgos muestran que, cuando se gestiona de manera centralizada y estratégica, el AD permite optimizar la administración de identidades, consolidar recursos tecnológicos y garantizar trazabilidad en los procesos, reduciendo redundancias y vulnerabilidades críticas.

Desde una perspectiva práctica, los resultados sugieren que las instituciones públicas pueden fortalecer sus capacidades de planificación tecnológica y control interno mediante la integración del AD en sus estructuras organizacionales, alineándolo con estándares internacionales de seguridad y buenas prácticas de gestión de TI. Teóricamente, el estudio amplía la comprensión del AD más allá de su función operativa, posicionándolo como un instrumento estratégico de articulación organizacional que contribuye al desarrollo del gobierno digital y al cumplimiento de objetivos institucionales más amplios.

Asimismo, la investigación abre oportunidades para futuras líneas de estudio, incluyendo el análisis de algoritmos de seguridad avanzados, la integración con tecnologías emergentes de automatización y la evaluación del impacto de estas soluciones en la eficiencia y resiliencia de los procesos administrativos.

En conclusión, los resultados confirman que la implementación estructurada y estratégica del Active Directory no solo cumple con los objetivos planteados al inicio del estudio, sino que también proporciona un marco sólido para fortalecer la modernización tecnológica del Estado, promoviendo eficiencia, seguridad y gobernanza sostenible en el ámbito público.

REFERENCIAS

Acosta Luis, D., Rodríguez López, W. A., Peñaherrera Larenas, M. F., García Hevia, S., y La O Mendoza, Y. (2021). Metodología de la investigación en la educación superior. Revista Universidad y Sociedad, 13(4), 283–293.

Álvarez, R. M., Garma Quen, P. M., Yanez Nava, D., Guillen-Morales, M. M., y Novelo Pérez, M. I. (2021). Validación de un cuestionario para determinar valores asociados al consumo de maíz. Journal of Negative and No Positive Results, 6(9), 1171–1180. https://doi.org/10.19230/jonnpr.4021

Auditoría Superior de la Federación. (2021). Informe del resultado de la fiscalización superior de la Cuenta Pública. https://www.asf.gob.mx

Axelos. (2019). ITIL® Foundation: ITIL 4 Edition. TSO (The Stationery Office).

Bendezú López, G. R., y Ramos Solano, G. (2024). Implementación del Active Directory para la optimización de la Infraestructura de Red en el Poder Judicial. https://repositorio.utp.edu.pe/handle/20.500.12867/8746

Caballero Álvarez, J. (2023). Despliegue, vulnerabilidades y protección de un directorio activo (Universidad Oberta de Catalunya). https://openaccess.uoc.edu/bitstream/10609/147405/4/jcaballero3TFG0123m emoria.pdf

Camavilca-Vega , D. . (2025). Inteligencia de negocios en la educación. Una revisión sistemática de literatura . 593 Digital Publisher CEIT, 10(2), 335-348. https://doi.org/10.33386/593dp.2025.2.2698

Canadian Centre for Cyber Security. (2023, December 12). Practitioner guidance for securing Microsoft Active Directory services in your organization: ITSP.60.100. https://www.cyber.gc.ca/en/guidance/practitioner-guidance-securing-microsoft-active-directory-services-your-organization-itsp60100

CCN-CERT. (2023). Informe anual de ciberamenazas y tendencias. Centro Criptológico Nacional. https://www.ccn-cert.cni.es/es/informes/informes-ccncert-publicos/6338-ccn-cert-ia-13-21-ciberamenazas-y-tendencias-edicion-2021-1/file?format=html

Centro Nacional de Seguridad Digital. (2022). Reporte anual de incidentes de seguridad digital en el sector público. https://www.gob.pe/institucion/cnsd/informes

Cordero Guzman, D., y Ramón Poma, G. (2021). Modelo tecnológico e infraestructura informática de un campus virtual para el contexto universitario. Revista Científica Y Tecnológica UPSE, 8(2), 48-58. https://doi.org/10.26423/rctu.v8i2.627

Diksha, Goel, D., Ward, M., Neumann, A., Neumann, F., Nguyen, H., y Guo, M. (2023). Defending Active Directory by Combining Neural Network Based Dynamic Program and Evolutionary Diversity Optimisation [Preprint]. University of Adelaide. https://arxiv.org/abs/2204.03397

FDIC Office of Inspector General. (2023). The FDIC's Security Controls Over Microsoft Windows AD. https://www.fdicoig.gov/sites/default/files/reports/2023-03/AUD-23-002Redacted.pdf

Echeverri, D. (2024). Curso Hacking sobre Active Directory. Aula Virtual de Vitae. https://www.vitaedigital.com/download/h5axrus36f3vzt0m7vxd37pjgbutup/F0000001841_curso_hacking_sobre_active_directory_aula_virtual.pdf

Fernández, V. H. (2020). Tipos de justificación en la investigación científica. Espíritu Emprendedor 4(3), 65–76. https://doi.org/10.33970/eetes.v4.n3.2020.207

Goel, D., Neumann, A., Neumann, F., Nguyen, H., y Guo, M. (2023). Scalable edge blocking algorithms for defending Active Directory style attack graphs. arXiv. https://arxiv.org/abs/2212.04326

Guevara Sandoval, N. A. (2024). Sistema de monitoreo de infraestructura de TI para soporte a la gestión de recursos de la Oficina de Tecnologías de la Información. https://repositorio.unc.edu.pe/handle/20.500.14074/6712

Guo, M., Li, J., Neumann, A., Neumann, F., y Nguyen, H. (2021). Practical fixedparameter algorithms for defending Active Directory style attack graphs. arXiv. https://doi.org/10.48550/arXiv.2112.13175

Hadi, M. M., Martel, C. P., Huayta, F. T., Rojas, C. R., y Arias, J. L. (2023). Metodología de la investigación: Guía para el proyecto de tesis. Instituto Universitario de Innovación Ciencia y Tecnología Inudi Perú. https://doi.org/10.35622/inudi.b.073

Hafzullah, I. (2024). A novel approach to enhancing Active Directory security in academic institutions. Balkan Journal of Electrical y Computer Engineering, 12(4), 393–402. https://doi.org/10.17694/bajece.1567393

Hernández Suárez, C. A., Prada Núñez, R., y Gamboa Suárez, A. A. (2021). Gestión tecnológica estratégica: uso del ecosistema de la web social 2.0 en educación superior. Revista Venezolana De Gerencia, 26(Número Especial 5), 77-92. https://doi.org/10.52080/rvgluz.26.e5.6

Huy, Q. N., Guo, M., y Nguyen, H. X. (2024). Optimizing cyber response time on temporal Active Directory networks using decoys (Extended Version). Proceedings of the ACM Conference. https://doi.org/10.1145/nnnnnnn.nnnnnnn

INEI (2022). Diagnóstico de capacidades tecnológicas en el sector público. https://www.inei.gob.pe

Manrique Leiva, K. M. (2025). Implementación de la herramienta Active Directory y la organización tecnológica en la Empresa EMAPA Huaral S.A. UNJFSC. https://repositorio.unjfsc.edu.pe/handle/20.500.14067/10677

Mendoza Munguía, L. D., y Zelada Pérez, J. A. (2022). Propuesta de implementación de una infraestructura en Azure para automatizar los servicios de los clientes en la empresa Multimarkas S.A.C. https://alicia.concytec.gob.pe/vufind/Record/UTPD_220c23523b6b4548c801c 2f1ba479395

Montero Caro, M. D. (2021). Educación, Gobierno Abierto y progreso: los Objetivos de Desarrollo Sostenible (ODS) en el ámbito educativo. Una visión crítica de la LOMLOE. Revista de Educación y Derecho, (23), 1–26. https://doi.org/10.1344/REYD2021.23.34443

Monzón Munguía, P. A. (2022). Rediseño e implementación del directorio activo para mejorar la administración de usuarios y recursos en el HDAC http://repositorio.undac.edu.pe/handle/undac/2908

Ngo, H. Q., Guo, M., y Nguyen, H. (2024). Optimizing cyber response time on temporal Active Directory networks using decoys. arXiv. https://arxiv.org/abs/2403.18162

Ocrospoma, W., y Romero, H. (2021). Sistema web para el proceso de incidencias en la empresa RR&C Grupo Tecnológico S.A.C. 3C TIC. Cuadernos de desarrollo aplicados a las TIC, 10(1), 43-67. https://doi.org/10.17993/3ctic.2021.101.4367

Peña Casanova, M., y Anías Calderón, C. (2020). Modelo para la gestión de infraestructuras de tecnologías de la información. Tecnológicas, 23(48), 31–53. https://doi.org/10.22430/22565337.1449

Romero, J., Pérez, M., y Delgado, R. (2021). Metodología de la investigación. Editorial Universitaria.

Ronquillo Bolaños, C., Ballesteros López, L., Vera Loor, R., y Román Ordoñez, F. (2024). Teoría General de Sistemas, supuestos subyacentes y no subyacentes para el crecimiento económico empresarial. ULEAM Bahía Magazine, 5(9), 70–78. https://doi.org/10.56124/ubm.v5i9.010

Vásquez Ramírez, A. A., Guanuchi Orellana, L. M., Cahuana Tapia, R. D., Vera Treves, R. M., y Holgado Tisoc, J. (2023). Métodos de investigación científica. Instituto Universitario de Innovación Ciencia y Tecnología Inudi Perú. https://doi.org/10.35622/inudi.b.094

Yuhang, D., y He, R. (2023). Research on the public sector's strategic management process based on dynamic capabilities. International Journal of Science and Research Archive, 10(1), 469-477. https://doi.org/10.30574/ijsra.2023.10.1.0769