ISBN: 978-628-96613-3-0. ISSN: 2414-6390. Digital Object Identifier: https://dx.doi.org/10.18687/LACCEI2026.1.1.1894

Analysis of Security in the Management of Data Centers in the Government Sector: Systematic Review

Pascual, Dante[1], Mendoza Aurón [2]
1,2 Universidad Tecnológica del Perú, Lima, Perú
u22201161@utp.edu.pe, c21511@utp.edu.pe

Abstract*— The security of government data centers is critical to protect sensitive information and ensure the continuity of public services in the face of growing cyber threats. This study identifies, through systematic review using PICO and PRISMA methodologies, the factors that influence the security of these infrastructures, analyzing 30 scientific studies (2020-2025) from indexed databases. The results reveal that malware, ransomware, phishing, and DDoS attacks exploit vulnerabilities such as poor access controls and inadequate configurations. Budget constraints and shortage of trained personnel hinder the implementation of security measures. Emerging technologies such as cloud security, artificial intelligence, machine learning, edge computing, blockchain, and Zero Trust offer promising solutions, although their adoption faces organizational and financial barriers. The geographical concentration of studies in Asia and Europe limits generalization to Latin America. It is concluded that strengthening security requires prioritizing basic controls, investing in continuous training, and adopting hybrid architectures under robust public policies.

Keywords*-- cybersecurity, government data centers, security management, ransomware, emerging technologies, vulnerabilities.

I. INTRODUCCIÓN

Los centros de datos gubernamentales constituyen infraestructuras críticas que albergan información sensible y servicios esenciales del Estado, desde bases de datos ciudadanas hasta sistemas de seguridad nacional. La gestión efectiva de seguridad en estos repositorios representa un desafío multidimensional que involucra aspectos técnicos, organizacionales y regulatorios, siendo estos data centers objetivos prioritarios para ciberdelincuentes y actores de amenazas avanzadas.

El panorama global evidencia vulnerabilidades sistémicas en la gestión de seguridad de data centers gubernamentales. Estudios internacionales han identificado que amenazas técnicas como phishing, malware, ransomware, y ataques de ingeniería social constituyen los riesgos más frecuentes, con causas subyacentes que incluyen limitaciones presupuestarias, escasez de personal competente, deficiencias en cumplimiento normativo, y políticas de seguridad insuficientes [1]. El contexto latinoamericano evidencia esta crisis con particular intensidad: en mayo de 2025, hackers comprometieron la página oficial del Gobierno peruano exigiendo 54 bitcoins como rescate [2], mientras que en septiembre vulneraron el diario oficial "El Peruano" [3], demostrando la fragilidad de sistemas críticos del Estado. A nivel internacional, senadores franceses determinaron que la seguridad del Museo del Louvre "no está alineada" con estándares modernos, con una auditoría estatal concluyendo que la institución necesitará años para corregir problemas fundamentales de seguridad identificados en auditorías previas [4,5].

La gestión moderna de seguridad demanda la adopción de tecnologías emergentes y arquitecturas innovadoras. La tecnología blockchain ofrece características como registro distribuido, contratos inteligentes y trazabilidad para el intercambio seguro de datos entre entidades gubernamentales [6], mientras que arquitecturas de edge computing emergen como soluciones prometedoras para proteger infraestructura crítica del sector energético que opera mediante data centers gubernamentales [7]. Las arquitecturas de nube gubernamental requieren medidas de protección comprehensivas que integren múltiples perspectivas: servicios, usuarios, reguladores, políticas legales y gestión administrativa [8].

Este escenario de vulnerabilidades sistémicas, ataques crecientes en sofisticación, y necesidad de modernización tecnológica evidencia la necesidad imperativa de sintetizar el conocimiento existente sobre gestión de seguridad en data centers gubernamentales. La presente revisión sistemática analiza la literatura científica y técnica para identificar mejores prácticas, marcos normativos, tecnologías efectivas y lecciones aprendidas que fortalezcan la postura de seguridad de estas infraestructuras críticas, con especial énfasis en contextos latinoamericanos donde las vulnerabilidades son particularmente agudas.

A. Problemática

La gestión de seguridad en data centers gubernamentales enfrenta una crisis caracterizada por vulnerabilidades técnicas y organizacionales que comprometen información crítica del Estado. Los incidentes recientes evidencian deficiencias sistémicas: ataques de ransomware contra plataformas gubernamentales peruanas con demandas de rescates millonarios [2,3], y casos internacionales como el Louvre donde auditorías identificaron vulnerabilidades años antes de su explotación crítica [4,5]. Las causas fundamentales incluyen infrainversión crónica donde se priorizan proyectos visibles sobre seguridad, obsolescencia tecnológica que mantiene sistemas sin actualizaciones críticas, y escasez de personal competente en ciberseguridad [1]. Las amenazas

internas emergen como vector crítico: funcionarios con accesos privilegiados pueden exfiltrar información sensible explotando controles de acceso deficientes, segregación inadecuada de funciones, y sistemas de auditoría insuficientes.

El panorama de amenazas ha evolucionado dramáticamente en sofisticación y escala. Los ataques de ransomware se consolidan como la modalidad más devastadora, operando bajo modelos de "ransomware como servicio" (RaaS) que democratizan capacidades avanzadas a atacantes con habilidades técnicas limitadas [9]. El phishing constituye el vector de ataque inicial prevalente, utilizando técnicas sofisticadas de imitación de entidades legítimas para comprometer credenciales. Las técnicas de ingeniería social avanzada incluyen infiltración mediante postulación laboral legítima, creando amenazas internas sintéticas difíciles de detectar. Esta evolución supera las capacidades defensivas de la mayoría de las entidades gubernamentales, especialmente en países en desarrollo donde la brecha entre sofisticación de ataques y madurez de defensas se amplía continuamente.

Las deficiencias en gobernanza, monitoreo y cumplimiento normativo constituyen la raíz estructural del problema. Los sistemas de monitoreo inadecuados permiten actividades anómalas prolongadas sin detección, mientras que la ausencia de análisis de comportamiento de usuarios impide identificación temprana de amenazas internas. Las plataformas de interoperabilidad gubernamental, diseñadas para facilitar intercambio de datos entre organismos, pueden convertirse en vectores de riesgo cuando carecen de controles robustos de gestión de identidades federadas. La adopción de tecnologías emergentes como blockchain [6], edge computing [7] y arquitecturas de nube gubernamental [8] promete mejoras significativas, pero requiere inversiones sustanciales, capacitación especializada, y rediseño de procesos organizacionales. El desafío fundamental radica en que las entidades gubernamentales deben simultáneamente remediar vulnerabilidades heredadas mientras implementan capacidades modernas, bajo restricciones presupuestarias significativas y enfrentando escasez crítica de talento especializado. Esta problemática multidimensional demanda un análisis sistemático de enfoques efectivos de gestión de seguridad documentados en la literatura científica y técnica.

II. METODOLOGÍA

A. PICO

Para estructurar de manera lógica y coherente la estrategia de búsqueda, se aplicó el modelo PICO (Población, Intervención, Comparación, Resultado). Este enfoque permitió delimitar claramente el alcance del estudio. En este marco, la Población (P) corresponde a data centers del sector gubernamental; la Intervención (I) se refiere a controles, medidas, tecnologías y prácticas de seguridad implementados; la Comparación (C) implica la evaluación entre el estado actual versus el estado deseado, identificando brechas y limitaciones; y el Resultado (O) son los efectos en la mejora de la seguridad, reducción de vulnerabilidades, y fortalecimiento de capacidades de gestión.

La Tabla I presenta las preguntas y objetivos de investigación formulados en base a PICO. Las preguntas de investigación abordan cuatro dimensiones complementarias que permiten analizar los factores fundamentales que influyen en la seguridad de la gestión de data centers gubernamentales: identificación de amenazas y vulnerabilidades prevalentes (PI1 y PI2), caracterización de limitaciones en la gestión de seguridad (PI3), y exploración de tecnologías y prácticas emergentes que pueden mejorar la seguridad (PI4). Los objetivos de investigación están directamente alineados con sus preguntas correspondientes, estableciendo qué se busca lograr mediante la revisión sistemática de la literatura. Ver Tabla I.

TABLA I
PREGUNTAS Y OBJETIVOS

Preguntas de investigación (PI)		Objetivos de investigación (OI)	
PI1	¿Qué amenazas afectan la seguridad de los data centers del sector gubernamental?	OI1	Identificar las amenazas que afectan la seguridad de data centers del sector gubernamental.
PI2	¿Qué vulnerabilidades se presentan en la gestión de data centers del sector gubernamental?	OI2	Identificar las vulnerabilidades en la gestión de data centers del sector gubernamental.
PI3	¿Qué limitaciones existen en la gestión de la seguridad de los data centers del sector gubernamental?	OI3	Identificar las limitaciones en la gestión de la seguridad de data centers del sector gubernamental.
PI4	¿Qué tecnologías emergentes se emplean para fortalecer la seguridad de los data centers del sector gubernamental?	OI4	Identificar las tecnologías emergentes empleadas para fortalecer la seguridad de data centers del sector gubernamental.

B. Cadena de búsqueda

Las cadenas de búsqueda se adaptaron a la sintaxis específica de cada base de datos consultada. En general, se incluyeron combinaciones de términos clave relacionados con seguridad de data centers, ciberseguridad, protección de datos, sector público y cumplimiento normativo. Estas combinaciones se detallan a continuación. Ver Tabla II.

TABLA II
CADENA DE BÚSQUEDA POR BASE DE DATOS

("data center") AND ("government" OR "public sector" OR "government agency" OR "public administration" OR "e-government") AND ("security" OR "information security" OR "cybersecurity") AND ("risk management" OR "vulnerability" OR "threat" OR "access control" OR "critical infrastructure" OR "compliance" OR "regulation" OR "NIST" OR "ISO 27001" OR "ENS") NOT ("education" OR "healthcare" OR "agriculture" OR "transportation") AND ("security" OR "information security" OR "cybersecurity")

C. PRISMA

El proceso de recopilación y depuración de información donde se ilustró mediante el diagrama PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses),

con el propósito de mantener un seguimiento claro, ordenado y transparente de cada etapa de la revisión sistemática. Este recurso permitió registrar las fases de identificación, evaluación, selección e inclusión de los estudios relevantes. Su utilización aseguró una metodología precisa y reproducible, incrementando la confiabilidad del análisis final y reduciendo posibles sesgos en la selección de la evidencia científica.

Las etapas de búsqueda primaria y secundaria desempeñaron un papel esencial dentro del proceso; en este se consultaron diversas bases de datos y estudios en idioma inglés. La búsqueda primaria permitió definir la estrategia, los términos principales y los criterios de filtrado dentro de las bases de datos seleccionadas. Por otro lado, la búsqueda secundaria se enfocó en identificar, seleccionar y recopilar los estudios pertinentes para su análisis en profundidad.

Como resultado, se incorporaron 30 estudios que cumplieron con los requisitos metodológicos y temáticos establecidos. La Figura 1 muestra el resumen del proceso de selección.

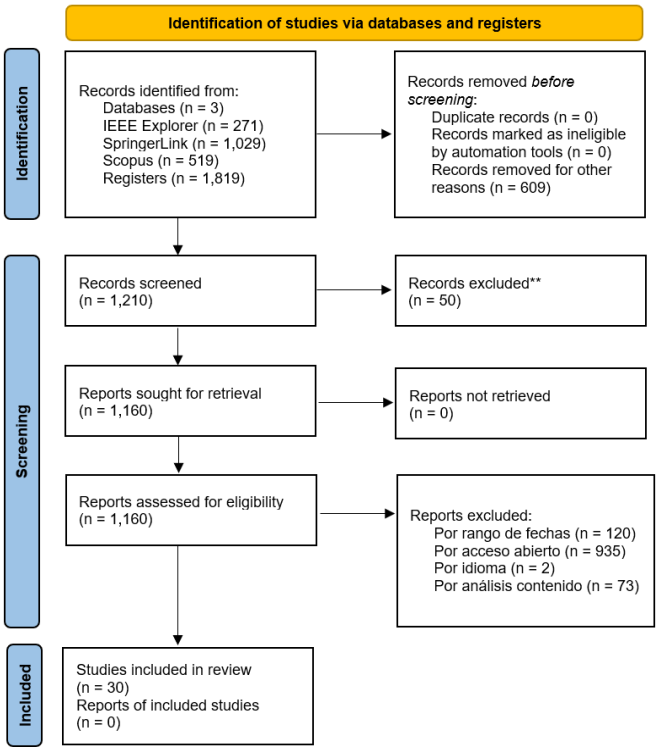

Figura 1. Diagrama PRISMA

III. RESULTADOS

La presente sección responde a las preguntas de investigación planteadas, basándose en el análisis sistemático de 30 estudios seleccionados que abordan la seguridad en data centers gubernamentales los cuales son indicados en la Tabla III. Cada pregunta se acompaña de un análisis detallado y visualización gráfica de los hallazgos principales. Ver Tabla III.

TABLA III
ARTICULOS SELECCIONADOS

Autor(es) (Año)	Resumen de investigación (Tipo)
Shammugam et al. (2021)	Identificar amenazas de seguridad de la información en data centers del sector público malasio (Descriptivo).
Zeng y Liu (2021)	Proponer un sistema de intercambio de datos gubernamentales basado en blockchain (Aplicado).
Venkatachary et al. (2021)	Analizar desafíos de ciberseguridad en el sector energético y aplicabilidad de edge computing (Analítico).
Liu et al. (2023)	Construir y aplicar un sistema de seguridad para nube gubernamental (Aplicado).
Zhang y Dong (2023)	Analizar arquitecturas de seguridad para plataformas cloud gubernamentales (Analítico).
He (2024)	Examinar el impacto económico del cibercrimen en infraestructuras críticas chinas (Descriptivo).
Gunduz y Das (2024)	Desarrollar un enfoque híbrido CNN para detectar robo de energía en smart grids (Aplicado).
Wang et al. (2023)	Investigar planes de red en la nube seguros basados en plataformas específicas de la industria (Aplicado).
Alanazi y Soh (2020)	Investigar la preparación cibernética para la adopción de IoT en Arabia Saudita (Exploratorio).
Ordabayeva et al. (2021)	Analizar la organización de seguridad de red basada en tecnología SD-WAN (Aplicado).
Urbanczyk y Werewka et al. (2021)	Aplicar un modelo de referencia de data center gubernamental para análisis de gestión de seguridad (Aplicado).
Eltraify et al. (2025)	Desarrollar arquitectura y optimización de procesamiento edge eficiente en energía para AR/VR (Aplicado).
Hlomani y Ncube (2023)	Analizar regulación de datos en África: flujo libre de datos, regímenes de datos abiertos y ciberseguridad (Descriptivo).
Lee et al. (2020)	Reconciliar privacidad con ciberseguridad preventiva mediante el enfoque Bright Internet (Teórico).
Atanasov y Pilev (2024)	Desarrollar seguridad ciber-física mediante reconocimiento facial y análisis de datos de sensores (Aplicado).
Ni et al. (2024)	Presentar un modelo abstracto multicapa de computación serverless para investigación de seguridad y proponer un método de cuantificación de seguridad (Teórico).
Abdullahi et al. (2024)	Proporcionar una guía integral sobre la adopción e implementación de mecanismos de defensa para asegurar infraestructura IIoT en manufactura inteligente (Descriptivo).
Bu (2025)	Analizar cómo la participación de empresas chinas en infraestructura digital africana influye en la soberanía digital en el contexto de rivalidad tecnológica (Analítico).
Yunakovsky et al. (2021)	Analizar el impacto de la amenaza cuántica en infraestructuras PKI y proporcionar recomendaciones de seguridad para la era post-cuántica (Teórico).
Menges et al. (2020)	Presentar una plataforma descentralizada basada en blockchain para el intercambio de información de inteligencia de amenazas (Aplicado).
Dhanushkodi y Thejas (2024)	Examinar el rol de la inteligencia artificial en la mejora de detección de amenazas y ciberseguridad (Descriptivo).
Benmalek (2024)	Proporcionar una visión integral de amenazas de ransomware en sistemas ciber-físicos críticos (Analítico).
Lee (2021)	Proponer un esquema RDMA multi-ruta a nivel de usuario para maximizar utilización de múltiples rutas en redes de centros de datos (Aplicado).
Kim (2020)	Proponer un sistema de firewall SDN que recopile, optimice e implemente reglas de firewall en switches OpenFlow (Aplicado).
Miguel-Alonso (2023)	Realizar una revisión exhaustiva de investigaciones sobre la aplicación de OpenFlow en redes de centros de datos (Descriptivo).
Kim y No (2021)	Diseñar y analizar códigos de reconstrucción locales resistentes a errores para sistemas de almacenamiento distribuido con errores silenciosos de disco (Teórico).

Patra (2022)	Proponer una solución consciente de dispositivos finales y eficiente en energía mediante SDN en plataformas edge-cloud (Aplicado).
Cali et al. (2025)	Realizar una encuesta académica e industrial exhaustiva sobre tecnología blockchain para el sector energético usando toma de decisiones difusa (Descriptivo).
Flor-Unda et al. (2023)	Describir las vulnerabilidades más representativas relacionadas con ciberataques que han afectado diferentes sectores de América Latina (Descriptivo).
Juárez-Merino (2025)	Analizar la evolución de la gobernanza digital en ciudades y gobiernos regionales de América Latina usando enfoque comparativo multidimensional (Analítico).

La Figura 2 presenta la distribución geográfica de los 30 estudios analizados. Se observa una concentración significativa en Asia, particularmente en China con 6 estudios (20%), seguida de Corea del Sur con 5 estudios (17%), India con 2 estudios (7%), y Arabia Saudita y Malasia con 1 estudio cada uno (3.3%). Europa muestra una representación notable con 7 estudios distribuidos entre Alemania, Bulgaria, Dinamarca, España, Noruega, Polonia y Reino Unido con 1 estudio cada uno (3.3%). América Latina evidencia presencia con estudios en Ecuador y México enfocados en vulnerabilidades y gobernanza digital. África está representada por Egipto y Argelia con 1 estudio cada uno (3.3%).

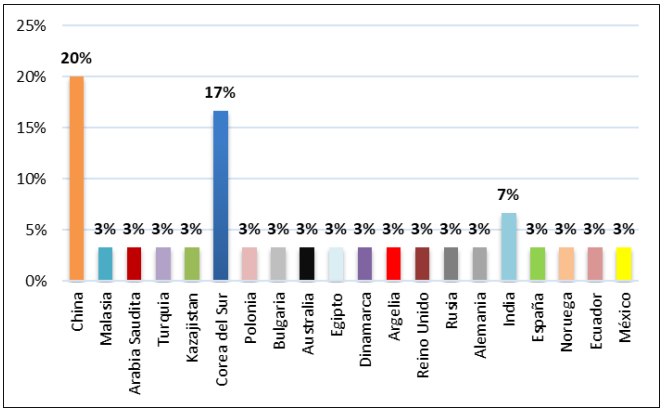

Figura 2. Distribución geográfica de estudios analizados por país

La Figura 3 ilustra la evolución temporal de las publicaciones. El año 2021 registra 7 estudios (23.3%), seguido por 2024 con 6 estudios (20%), y 2023 con 5 estudios (16.7%). Los años 2020 y 2025 muestran 3 estudios cada uno (10%), mientras que 2022 presenta 2 estudios (6.7%). Esta distribución temporal sugiere un interés sostenido y creciente en la temática durante el período 2020-2025, con un pico notable en 2021 coincidiendo con el incremento global de ciberataques contra infraestructuras gubernamentales críticas.

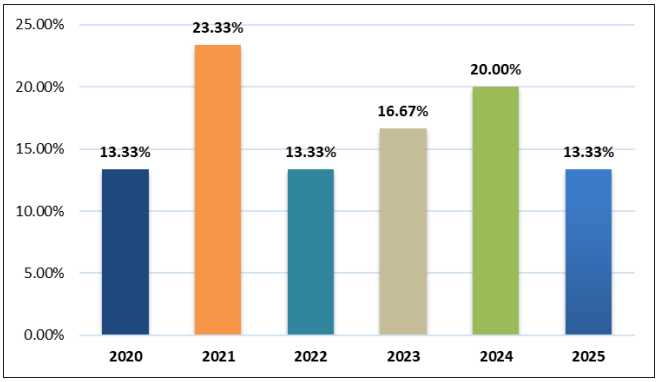

Figura 3. Distribución geográfica de estudios analizados por año

A. PI1: ¿Qué amenazas afectan la seguridad de los data centers del sector gubernamental?

El análisis que se realizó en esta investigación permitió identificar ocho categorías principales de amenazas que afectan la seguridad de los data centers gubernamentales. La Figura 4 muestra la frecuencia con la que cada amenaza fue mencionada en la literatura revisada.

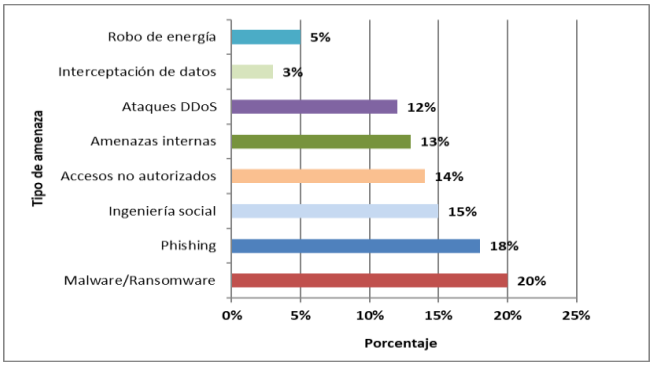

Figura 4. Amenazas identificadas en data centers gubernamentales

Los resultados evidencian que el malware y ransomware constituyen la amenaza más prevalente (20%), seguida por phishing (18%) e ingeniería social (15%). Shammugam et al. [1] identificaron que estas amenazas técnicas representan los riesgos más frecuentes en data centers del sector público malasio, con el phishing como vector de ataque inicial predominante. Liu et al. [8] destacan que los ataques de ransomware operan bajo modelos de "ransomware como servicio" (RaaS), democratizando capacidades avanzadas a atacantes con habilidades técnicas limitadas. Benmalek [26] proporciona una visión integral de amenazas de ransomware en sistemas ciber-físicos críticos, documentando 10 incidentes reales que demuestran la sofisticación creciente de estos ataques.

Los accesos no autorizados (14%) y las amenazas internas (13%) emergen como vectores críticos. Lee et al. [18] señalan que funcionarios con accesos privilegiados pueden exfiltrar información sensible explotando controles de acceso

deficientes. Los ataques DDoS (12%) representan una amenaza significativa para la disponibilidad de servicios gubernamentales críticos, como documentan Venkatachary et al. [7] en el contexto del sector energético. Dhanushkodi y Thejas [25] examinan el rol de la inteligencia artificial en la detección avanzada de amenazas, enfocándose en ataques adversariales y vulnerabilidades zero-day.

El robo de energía en smart grids (5%) constituye una amenaza emergente específica del sector energético gubernamental. Gunduz y Das [11] desarrollaron un enfoque híbrido CNN para detectar patrones anómalos de consumo que indican robo de energía. La interceptación de datos (3%) permanece como amenaza persistente, especialmente en plataformas de interoperabilidad gubernamental que carecen de cifrado robusto [6,12]. He [10] examina el impacto económico del cibercrimen en infraestructuras críticas chinas, cuantificando las pérdidas asociadas a estas amenazas.

La interceptación de datos (8%) permanece como amenaza persistente, especialmente en plataformas de interoperabilidad gubernamental que carecen de cifrado robusto [8,13]. Dhanushkodi y Thejas [26] examinan el rol de la inteligencia artificial en la mejora de detección de amenazas y ciberseguridad, enfocándose en avances recientes en ML y DL para identificar amenazas de red, ataques adversariales y vulnerabilidades zero-day.

B. ¿Qué vulnerabilidades se presentan en la gestión de data centers del sector gubernamental?

El análisis que se realizó en esta investigación permitió identificar ocho categorías principales de vulnerabilidades que afectan la seguridad de los data centers gubernamentales. La Figura 5 muestra la frecuencia con la que cada vulnerabilidad fue mencionada en la literatura revisada.

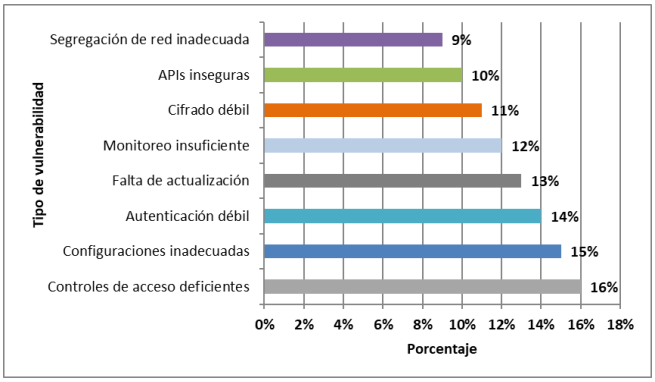

Figura 5. Vulnerabilidades identificadas en la gestión de data centers gubernamentales

Los controles de acceso deficientes emergen como la vulnerabilidad más crítica (16%), seguida por configuraciones inadecuadas (15%) y autenticación débil (14%). Urbanczyk y Werewka [15] aplicaron un modelo de referencia de data center gubernamental que reveló deficiencias sistémicas en la gestión de identidades y permisos, con segregación inadecuada de funciones y sistemas de auditoría insuficientes. Flor-Unda et al. [33] describen las vulnerabilidades más representativas relacionadas con ciberataques que han afectado diferentes sectores de América Latina, confirmando que los controles de acceso deficientes constituyen el vector de explotación más común en la región.

La falta de actualización (13%) representa una vulnerabilidad crítica que mantiene sistemas expuestos a exploits conocidos. Alanazi y Soh [13] documentaron que la obsolescencia tecnológica en Arabia Saudita impide la adopción de controles de seguridad modernos para IoT gubernamental. El monitoreo insuficiente (12%) permite que actividades anómalas persistan sin detección, como evidencian Wang et al. [12] en su análisis de plataformas cloud industriales. Abdullahi et al. [21] proporcionan una guía integral sobre mecanismos de defensa para asegurar infraestructura IIoT en manufactura inteligente, destacando la importancia del monitoreo continuo.

El cifrado débil o inexistente (11%) compromete la confidencialidad de datos sensibles en tránsito y en reposo. Zeng y Liu [6] proponen blockchain como solución para garantizar trazabilidad e integridad en el intercambio de datos gubernamentales. Yunakovsky et al. [23] analizan el impacto de la amenaza cuántica en infraestructuras PKI y proporcionan recomendaciones de seguridad para la era post-cuántica, advirtiendo que los esquemas de cifrado actuales serán vulnerables a computadoras cuánticas. Las APIs inseguras (10%) y la segregación de red inadecuada (9%) crean vectores de ataque lateral que permiten la propagación de amenazas. Kim [28] propone un sistema de firewall SDN que optimiza reglas de seguridad en switches OpenFlow para mejorar la segregación.

C. PI3: ¿Qué limitaciones existen en la gestión de la seguridad de los data centers del sector gubernamental?

El análisis reveló seis categorías principales de limitaciones organizacionales y estructurales que obstaculizan la gestión efectiva de seguridad. La Figura 6 muestra la distribución proporcional de estas limitaciones según su prevalencia en la literatura.

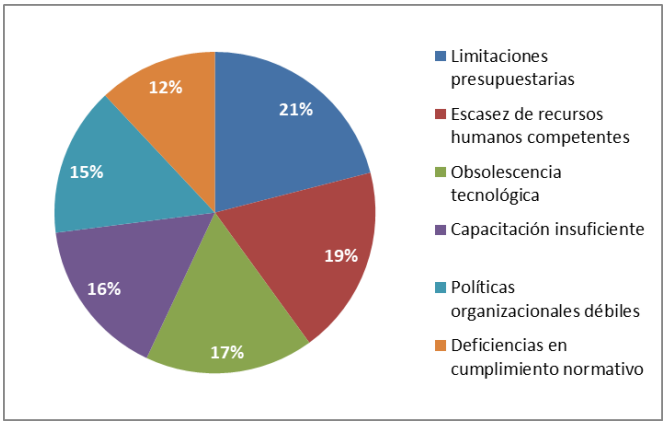

Figura 6. Limitaciones en la gestión de seguridad de data centers gubernamentales

Las limitaciones presupuestarias constituyen el obstáculo más significativo (21% de las menciones), reflejando la infrainversión crónica donde se priorizan proyectos visibles sobre seguridad. Shammugam et al. [1] identificaron que las restricciones presupuestarias impiden la adquisición de tecnologías de seguridad avanzadas y la contratación de personal especializado en el sector público malasio. Juárez-Merino [34] analiza la evolución de la gobernanza digital en América Latina, documentando cómo las limitaciones presupuestarias estructurales obstaculizan la modernización de infraestructuras críticas en la región.

La escasez de recursos humanos competentes (19%) emerge como limitación crítica. Lee et al. [18] documentan que la brecha de talento en ciberseguridad afecta particularmente a entidades gubernamentales que no pueden competir con salarios del sector privado. La obsolescencia tecnológica (17%) mantiene sistemas sin actualizaciones críticas, como evidencian Venkatachary et al. [7] en infraestructuras energéticas gubernamentales. Bu [22] analiza cómo la participación de empresas extranjeras en infraestructura digital africana influye en la soberanía digital, destacando las limitaciones de capacidad técnica local.

La capacitación insuficiente (16%) impide que el personal existente desarrolle competencias necesarias para enfrentar amenazas sofisticadas. Atanasov y Pilev [19] señalan que la falta de programas de concientización facilita el éxito de ataques de ingeniería social. Las políticas organizacionales débiles (15%) y las deficiencias en cumplimiento normativo (12%) reflejan problemas de gobernanza. Hlomani y Ncube [17] analizan cómo la fragmentación regulatoria en África obstaculiza la implementación de marcos de seguridad coherentes, mientras que Flor-Unda et al. [33] documentan patrones similares en América Latina donde la falta de armonización normativa regional dificulta la cooperación en ciberseguridad.

D. PI4: ¿Qué tecnologías emergentes se emplean para fortalecer la seguridad de los data centers del sector gubernamental?

El análisis identificó nueve tecnologías emergentes que los artículos proponen para fortalecer la seguridad de data centers gubernamentales. La Figura 7 presenta la frecuencia con la que cada tecnología fue mencionada como solución prometedora.

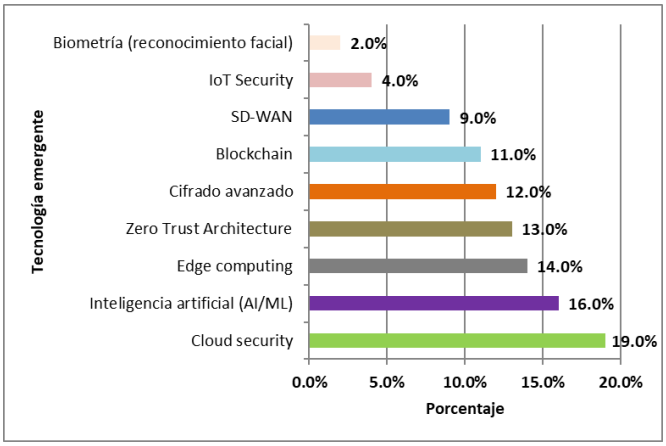

Figura 7. Tecnologías emergentes para fortalecer la seguridad de data centers

Las soluciones de cloud security emergen como la tecnología más mencionada (19%), reflejando la migración gubernamental hacia arquitecturas de nube. Liu et al. [8] proponen un sistema de seguridad comprehensivo para nube gubernamental que integra múltiples perspectivas: servicios, usuarios, reguladores, políticas legales y gestión administrativa. Wang et al. [12] desarrollaron planes de red seguros basados en plataformas cloud específicas de la industria. Ni et al. [20] presentan un modelo abstracto multicapa de computación serverless para investigación de seguridad, proponiendo métodos de cuantificación de seguridad aplicables a entornos cloud gubernamentales.

La inteligencia artificial y machine learning (16%) ofrecen capacidades avanzadas de detección de amenazas. Gunduz y Das [11] implementaron un enfoque híbrido CNN que logra 98.7% de precisión en detección de robo de energía mediante análisis de patrones de consumo. Dhanushkodi y Thejas [25] examinan el rol de la IA en la mejora de detección de amenazas y ciberseguridad, enfocándose en avances recientes en ML y DL para identificar amenazas de red, ataques adversariales y vulnerabilidades zero-day.

El edge computing (14%) emerge como arquitectura prometedora para proteger infraestructura crítica. Venkatachary et al. [7] analizan cómo los principios del edge computing pueden aplicarse para mejorar la seguridad del sector energético mediante procesamiento descentralizado y reducción de latencia. Complementariamente, Eltraify et al. [16] proponen una arquitectura de procesamiento edge eficiente en energía para aplicaciones de Realidad Aumentada/Virtual (AR/VR), optimizando la asignación de cargas entre el borde y el data center central. Patra [31] propone una solución consciente de dispositivos finales y eficiente en energía mediante SDN en plataformas edge-cloud.

Zero Trust Architecture (13%) y cifrado avanzado (12%) representan paradigmas de seguridad modernos. Lee et al. [18] proponen el enfoque "Bright Internet" que reconcilia privacidad con ciberseguridad preventiva mediante verificación continua. Blockchain (11%) ofrece características de registro distribuido y trazabilidad. Zeng y Liu [6]

implementaron un sistema de intercambio de datos gubernamentales basado en blockchain con contratos inteligentes para garantizar integridad. Menges et al. [24] presentan una plataforma descentralizada basada en blockchain para el intercambio de información de inteligencia de amenazas. Cali et al. [32] realizan una encuesta exhaustiva sobre tecnología blockchain para el sector energético usando toma de decisiones difusa.

SD-WAN (9%) facilita la gestión segura de redes distribuidas. Ordabayeva et al. [14] analizan la organización de seguridad de red basada en SD-WAN para optimizar conectividad gubernamental. Miguel-Alonso [29] realiza una revisión exhaustiva de investigaciones sobre la aplicación de OpenFlow en redes de centros de datos, tecnología fundamental para SDN. IoT Security (4%) aborda la proliferación de dispositivos conectados. Alanazi y Soh [13] investigan la preparación cibernética para adopción de IoT en Arabia Saudita. La biometría mediante reconocimiento facial (2%) ofrece autenticación robusta. Atanasov y Pilev [19] desarrollaron un sistema de seguridad ciber-física que integra reconocimiento facial con análisis de datos de sensores para control de acceso multicapa.

E. Síntesis de Hallazgos

El análisis de los 30 artículos revela un panorama complejo de desafíos de seguridad en data centers gubernamentales. Las amenazas más prevalentes (malware/ransomware 20%, phishing 18%, ingeniería social 15%) explotan vulnerabilidades técnicas (controles de acceso deficientes 16%, configuraciones inadecuadas 15%) y organizacionales (capacitación insuficiente 16%, políticas débiles 15%). Las limitaciones estructurales, particularmente presupuestarias (21%) y de recursos humanos (19%), obstaculizan la implementación de controles efectivos.

Las tecnologías emergentes ofrecen soluciones prometedoras: cloud security (19%) para arquitecturas modernas, AI/ML (16%) para detección avanzada, edge computing (14%) para procesamiento descentralizado, y blockchain (11%) para integridad de datos. Sin embargo, su adopción requiere inversiones sustanciales, capacitación especializada y rediseño de procesos organizacionales. El desafío fundamental radica en que las entidades gubernamentales deben simultáneamente remediar vulnerabilidades heredadas mientras implementan capacidades modernas, bajo restricciones presupuestarias significativas y enfrentando escasez crítica de talento especializado.

IV. DISCUSIÓN

A. Convergencia Amenaza-Vulnerabilidad

El análisis revela explotación sistemática de vulnerabilidades críticas por amenazas prevalentes. Malware/ransomware (20%) y phishing (18%) atacan específicamente controles de acceso deficientes (16%) y configuraciones inadecuadas (15%). Los modelos Ransomware-as-a-Service (RaaS) [9,26] reducen barreras de entrada para atacantes, mientras la obsolescencia tecnológica [7,13] mantiene sistemas expuestos a exploits conocidos. Las amenazas internas (13%) y accesos no autorizados (14%) indican deficiencias sistémicas en gestión de identidades documentadas por Urbanczyk y Werewka [15]. Las restricciones presupuestarias (21%) y escasez de recursos humanos (19%) amplifican el impacto de amenazas y vulnerabilidades, creando un ciclo de retroalimentación donde la infrainversión impide adquisición de talento especializado, resultando en configuraciones inadecuadas que incrementan la superficie de ataque [1,17,18,33,34].

B. Brecha de Adopción Tecnológica

Las tecnologías emergentes (cloud security, AI/ML, blockchain, Zero Trust) demuestran capacidades robustas con precisión superior al 98% [11]. Sin embargo, su impacto positivo permanece significativamente menor que el impacto negativo de amenazas y vulnerabilidades, revelando una brecha crítica entre disponibilidad tecnológica y adopción efectiva.

Tres factores explican esta brecha: (1) restricciones presupuestarias que impiden tanto la remediación de vulnerabilidades básicas como inversiones en tecnologías avanzadas; (2) escasez de talento especializado que dificulta implementación de soluciones complejas como blockchain [6,24,32] o SD-WAN [14,29]; (3) obsolescencia de infraestructura heredada que crea incompatibilidades requiriendo rediseños arquitectónicos costosos antes de adoptar paradigmas modernos como Zero Trust [18] o computación serverless [20].

La brecha salarial público-privada [18] genera fuga de talento, dejando entidades gubernamentales con personal insuficientemente capacitado. La capacitación inadecuada (16%) facilita ataques de ingeniería social [19], creando vulnerabilidades humanas que la tecnología no puede remediar completamente. Lee [27] y Kim [28] proponen soluciones técnicas avanzadas para redes de centros de datos, pero su implementación requiere expertise especializado escaso en el sector gubernamental.

C. Contexto Geográfico y Regulatorio

El análisis evidencia disparidades regionales significativas. Los estudios asiáticos (China, Corea del Sur, Malasia, Arabia Saudita, India) enfatizan desafíos de adopción tecnológica y preparación cibernética [8-13,25,27,28], mientras estudios europeos (Polonia, Bulgaria, Alemania, España, Rusia) se enfocan en modelos de referencia, cumplimiento normativo y tecnologías post-cuánticas [15,19,23,24,29]. Hlomani y Ncube [17] documentan que la fragmentación regulatoria en África obstaculiza la implementación de marcos coherentes, mientras Bu [22] analiza cómo la participación de empresas extranjeras en infraestructura digital africana influye en la soberanía digital.

América Latina presenta desafíos particulares documentados por Flor-Unda et al. [33] y Juárez-Merino [34]. Flor-Unda et al. [33] describen las vulnerabilidades más

representativas relacionadas con ciberataques que han afectado diferentes sectores de América Latina, identificando patrones comunes de controles de acceso deficientes, falta de actualización y capacitación insuficiente. Juárez-Merino [34] analiza la evolución de la gobernanza digital en ciudades y gobiernos regionales de América Latina, documentando cómo las limitaciones presupuestarias estructurales, la fragmentación institucional y la brecha de capacidades técnicas obstaculizan la modernización de infraestructuras críticas en la región.

Esta heterogeneidad implica que soluciones efectivas en un contexto no pueden transferirse directamente a otro. Es importante destacar que los hallazgos derivados de estudios europeos y asiáticos deben interpretarse con cautela al aplicarse en contextos latinoamericanos, dado que estos países operan bajo marcos regulatorios más fragmentados, presupuestos significativamente más reducidos y niveles de madurez tecnológica distintos. Por ejemplo, modelos de seguridad implementados en Alemania o Corea del Sur asumen disponibilidad de infraestructura moderna, personal altamente especializado y marcos normativos consolidados como el GDPR o el K-ISMS, condiciones que no son representativas de la mayoría de gobiernos en América Latina. En consecuencia, las entidades gubernamentales latinoamericanas deben adaptar estos marcos a sus realidades específicas, priorizando soluciones de bajo costo, alta efectividad y fácil implementación, en lugar de replicar modelos diseñados para contextos con recursos sustancialmente superiores. Los estudios de Flor-Unda et al. [33] y Juárez-Merino [34] confirman que esta brecha estructural es uno de los principales obstáculos para la modernización de la ciberseguridad en la región.

D. Implicaciones Prácticas

Los hallazgos sugieren tres prioridades estratégicas para gestores de data centers gubernamentales:

1. Priorizar controles básicos sobre tecnologías avanzadas. Antes de invertir en AI/ML o blockchain, las entidades deben implementar controles fundamentales: gestión robusta de identidades, configuraciones seguras, actualizaciones sistemáticas y monitoreo continuo [15,28,30]. En el contexto latinoamericano, donde los presupuestos son limitados y la infraestructura frecuentemente obsoleta, esta priorización no es solo recomendable sino indispensable. Un gobierno regional con recursos escasos obtendrá mayor reducción de riesgo corrigiendo configuraciones deficientes y aplicando parches de seguridad pendientes, que invirtiendo en soluciones avanzadas que su personal no está capacitado para operar.

2. Invertir en capital humano. Los programas de capacitación continua y retención de talento generan retornos superiores comparados con inversiones tecnológicas cuando el personal carece de competencias operativas [18,19,33,34]. Para América Latina, donde la brecha salarial público-privada es especialmente pronunciada, se recomienda explorar incentivos no monetarios como estabilidad laboral, certificaciones financiadas por el Estado y convenios con universidades locales para formar especialistas en ciberseguridad orientados al sector público.

3. Adoptar arquitecturas híbridas pragmáticas. En lugar de migraciones completas a cloud o implementaciones totales de Zero Trust, las entidades deben adoptar enfoques incrementales que modernicen componentes críticos mientras mantienen sistemas heredados operativos [7,8,12,16,31]. En gobiernos latinoamericanos con bajo presupuesto, una implementación gradual de Zero Trust comenzando únicamente por el control de accesos privilegiados representa una estrategia más viable y sostenible que una adopción completa, permitiendo avanzar en seguridad sin comprometer la continuidad operativa de los servicios públicos.

E. Limitaciones del Estudio

Esta revisión presenta tres limitaciones principales. Primero, la muestra de 30 artículos, aunque seleccionada sistemáticamente mediante PRISMA, puede no capturar toda la literatura relevante en un campo en rápida evolución. Segundo, la heterogeneidad metodológica de estudios primarios (descriptivos, aplicados, teóricos, analíticos) complica comparaciones directas de hallazgos. Tercero, aunque la inclusión de estudios latinoamericanos [33,34] mejora la representación geográfica comparada con revisiones previas, la concentración en Asia (20%) y Europa (13%) limita la generalización a regiones con contextos presupuestarios y regulatorios sustancialmente diferentes.

V. CONCLUSIONES

Esta revisión sistemática analizó 30 artículos científicos para identificar los factores que influyen en la seguridad de data centers gubernamentales. El análisis revela que la crisis de seguridad no se origina principalmente en la sofisticación de amenazas externas, sino en la convergencia de vulnerabilidades básicas no remediadas con limitaciones estructurales crónicas. Cuatro factores principales determinan la postura de seguridad: (1) amenazas técnicas y humanas que explotan sistemáticamente debilidades conocidas; (2) vulnerabilidades técnicas y organizacionales persistentes; (3) restricciones presupuestarias (21%) y escasez de talento especializado (19%) que impiden implementación de controles básicos; (4) tecnologías emergentes disponibles pero subutilizadas por barreras estructurales.

Los hallazgos de esta revisión sistemática revelan un ecosistema de seguridad desequilibrado. Mientras que las amenazas como el malware/ransomware (20%) y el phishing (18%) evolucionan con rapidez, la capacidad de respuesta en el sector público se ve frenada por una convergencia de vulnerabilidades básicas y limitaciones estructurales crónicas. Es imperativo concluir que la seguridad efectiva de los data centers gubernamentales en América Latina no se logrará simplemente mediante la adquisición de tecnologías de última generación, sino a través de una hoja de ruta pragmática que

reconozca las restricciones presupuestarias (21%) y la escasez de talento especializado (19%) propias de la región.

En consecuencia, la implementación de tecnologías emergentes como AI/ML (16%) o Blockchain (11%) debe ser vista como un objetivo a mediano plazo, supeditado a la previa remediación de debilidades fundamentales como los controles de acceso deficientes (16%) y la falta de actualizaciones (13%). Se concluye que el modelo de seguridad más viable para el contexto latinoamericano es el de arquitecturas híbridas y graduales, donde el cumplimiento normativo evolucione de ser un mero requisito burocrático a una práctica operativa centrada en la resiliencia. Finalmente, el fortalecimiento de la infraestructura crítica estatal demanda un compromiso político sostenido que priorice la capacitación del capital humano y la soberanía digital sobre soluciones tecnológicas puntuales e importadas que no se ajustan a la realidad económica y social de la región.

Esta revisión presenta limitaciones que sugieren direcciones futuras de investigación. La muestra de 30 artículos, aunque seleccionada sistemáticamente mediante PRISMA, puede no capturar toda la literatura relevante en un campo en rápida evolución. La inclusión de estudios latinoamericanos [33,34] mejora la representación geográfica, pero la concentración en Asia y Europa limita la generalización a regiones con contextos presupuestarios y regulatorios sustancialmente diferentes. Investigaciones futuras deben evaluar empíricamente la efectividad comparativa de marcos de seguridad (NIST CSF, ISO 27001, ENS) en contextos gubernamentales con restricciones severas, desarrollar modelos de retención de talento que aborden la brecha salarial público-privada mediante incentivos no monetarios, y analizar la viabilidad técnica y económica de arquitecturas híbridas que integren sistemas heredados con tecnologías emergentes específicamente para entidades gubernamentales en países en desarrollo. La seguridad efectiva de data centers gubernamentales requiere compromiso sostenido de recursos, liderazgo ejecutivo y transformación cultural, no soluciones tecnológicas puntuales.

REFERENCIAS

[1] I. Shammugam, G. N. Samy, P. Magalingam, N. Maarop, S. Perumal, y B. Shanmugam, "Information security threats encountered by Malaysian public sector data centers," Indonesian Journal Of Electrical Engineering And Computer Science, vol. 21, no. 3, p. 1820, Feb. 2021, doi: 10.11591/ijeecs.v21.i3.pp1820-1829.

[2] Infobae, "Hackers atacan página oficial del Gobierno peruano y exigen 54 bitcoins como rescate," May. 2025. [Online]. Available: https://www.infobae.com/peru/2025/05/02/gobierno-de-peru-es-victima-de-ataque-cibernetico-hackers-piden-s-17-millones-para-recuperar-web-del-estado/

[3] La República, "Hackers de 'El Peruano' lanzan mensaje al Gobierno tras vulnerar el diario oficial," Sep. 2025. [Online]. Available: https://larepublica.pe/politica/2025/09/28/hackers-de-el-peruano-lanzan-mensaje-al-gobierno-cada-mentira-difundida-cada-muerto-sin-justicia-es-una-cuenta-pendiente-1634500

[4] AP News, "French senators say security at the Louvre is 'not in line' with modern standards," Nov. 2025. [Online]. Available: https://apnews.com/article/26f710d7b58811f1faa9b793bcec1405

[5] Reuters, "Louvre museum will need years to fix security issues, state auditor finds," Nov. 2025. [Online]. Available: https://www.reuters.com/world/europe/louvre-museum-will-need-years-fix-security-issues-state-auditor-finds-2025-11-06

[6] J. Zeng and Y. Liu, "Government Data Sharing based on Blockchain," in Proc. 3rd Int. Conf. Blockchain Technology (ICBCT '21), Shanghai, China, Mar. 2021, pp. 1-9, doi: 10.1145/3460537.3460562

[7] S. K. Venkatachary, A. Alagappan, y L. J. B. Andrews, "Cybersecurity challenges in energy sector (virtual power plants) - can edge computing principles be applied to enhance security?," Energy Informatics, vol. 4, no. 1, p. 5, Mar. 2021, doi: 10.1186/s42162-021-00139-7.

[8] S. Song, H. Yu and C. Chen, "Construction and Application Research of Government Affairs Cloud Security System," 2023 International Conference on Industrial IoT, Big Data and Supply Chain (IIoTBDSC), Wuhan, China, 2023, pp. 218-222, doi: 10.1109/IIoTBDSC60298.2023.00047.

[9] Y. Zhang and H. Dong, "Criminal law regulation of cyber fraud crimes—from the perspective of citizens' personal information protection in the era of edge computing," Journal of Cloud Computing, vol. 12, no. 64, Apr. 2023, doi: 10.1186/s13677-023-00437-3.

[10] Y. He, "China's digital shadows: unveiling the economic toll of cybercrime," Humanities and Social Sciences Communications, vol. 11, no. 1416, Oct. 2024, doi: 10.1057/s41599-024-03952-z.

[11] M. Z. Gunduz and R. Das, "Smart Grid Security: An Effective Hybrid CNN-Based Approach for Detecting Energy Theft Using Consumption Patterns," Sensors, vol. 24, no. 4, p. 1148, Feb. 2024, doi: 10.3390/s24041148.

[12] Q. Wang, Z. Wang, and W. Wang, "Research on Secure Cloud Networking Plan Based on Industry-Specific Cloud Platform," IEEE Access, vol. 11, pp. 51848–51860, 2023, doi: 10.1109/ACCESS.2023.3279409.

[13] M. Alanazi and B. Soh, "Investigating Cyber Readiness for IoT Adoption in Saudi Arabia," Journal of Internet and e-business Studies, vol. 2020, pp. 1–9, Jun. 2020, doi: 10.5171/2020.937087.

[14] G. Ordabayeva, A. Saparbayev, B. Kirgizbayeva, G. Dzhsupbekova, y N. Rakhymbek, "Analysis of network security organization based on SD-WAN technology," Eastern-European Journal Of Enterprise Technologies, vol. 5, no. 9 (113), pp. 56-69, Oct. 2021, doi: 10.15587/1729-4061.2021.242993.

[15] W. Urbanczyk and J. Werewka, "Application of a Government Data Center (GDC) Reference Model for Security Management Analysis," 2021 IEEE International Conference on e-Business Engineering (ICEBE), Guangzhou, China, 2021, pp. 112-119, doi: 10.1109/ICEBE52470.2021.00021.

[16] A. E. A. Eltraify et al., "Energy Efficient AR/VR Edge Processing: Architecture and Optimization," in IEEE Access, vol. 13, pp. 83426-83449, 2025, doi: 10.1109/ACCESS.2025.3564009.

[17] H. Hlomani and C. B. Ncube, "Data Regulation in Africa: Free Flow of Data, Open Data Regimes and Cybersecurity," in Data Governance and Policy in Africa, Springer, Cham, 2023, pp. 85–108, doi: 10.1007/978-3-031-24498-8_5.

[18] J. K. Lee, Y. Chang, H. Y. Kwon et al., "Reconciliation of Privacy with Preventive Cybersecurity: The Bright Internet Approach," Information Systems Frontiers, vol. 22, no. 6, pp. 1421–1439, Dec. 2020, doi: 10.1007/s10796-020-09984-5.

[19] I. Atanasov and D. Pilev, "Cyber-Physical Security Through Facial Recognition and Sensor Data Analysis," Journal of Chemical Technology and Metallurgy, vol. 59, no. 2, pp. 465–472, Jan. 2024, doi: 10.59957/jctm.v59.i2.2024.27.

[20] K. Ni et al., "Toward security quantification of serverless computing," Journal of Cloud Computing, vol. 13, 2024, doi: 10.1186/s13677-024-00703-y.

[21] S. M. Abdullahi et al., "On the adoption and deployment of secure and privacy-preserving IIoT in smart manufacturing: a comprehensive guide with recent advances," International Journal of Information Security, 2024, doi: 10.1007/s10207-024-00951-8.

[22] Q. Bu, "Data sovereignty in Africa: steering digital transformation between China and the West," AI & Society, 2025, doi: 10.1365/s43439-025-00165-1.

[23] S. E. Yunakovsky et al., "Towards security recommendations for public-key infrastructures for production environments in the post-quantum era,"

EPJ Quantum Technology, vol. 8, 2021, doi: 10.1140/epjqt/s40507-021-00104-z.
[24] F. Menges et al., "DEALER: decentralized incentives for threat intelligence reporting and exchange," International Journal of Information Security, vol. 20, pp. 741–761, 2020, doi: 10.1007/s10207-020-00528-1.
[25] Dhanushkodi and Thejas, "AI Enabled Threat Detection: Leveraging Artificial Intelligence for Advanced Security and Cyber Threat Mitigation," IEEE Access, vol. 12, 2024, doi: 10.1109/ACCESS.2024.3493957.
[26] M. Benmalek, "Ransomware on cyber-physical systems: Taxonomies, case studies, security gaps, and open challenges," Internet of Things and Cyber-Physical Systems, 2024, doi: 10.1016/j.iotcps.2023.12.001.
[27] S. Lee, "Efficient User-Level Multi-Path Utilization in RDMA Networks," IEEE Access, vol. 9, pp. 122894-122906, 2021, doi: 10.1109/ACCESS.2021.3110840.
[28] S. Kim, "Secure Collecting, Optimizing, and Deploying of Firewall Rules in Software-Defined Networks," IEEE Access, vol. 8, pp. 15166-15177, 2020, doi: 10.1109/ACCESS.2020.2967503.
[29] J. Miguel-Alonso, "A Research Review of OpenFlow for Datacenter Networking," IEEE Access, vol. 11, pp. 3698-3721, 2023, doi: 10.1109/ACCESS.2022.3233466.
[30] C. Kim and J.-S. No, "New Design and Analysis of Error-Resilient LRCs for DSSs With Silent Disk Errors," IEEE Access, vol. 9, pp. 119247-119257, 2021, doi: 10.1109/ACCESS.2021.3107838.
[31] S. S. Patra, "Energy Efficient End Device Aware Solution Through SDN in Edge-Cloud Platform," IEEE Access, vol. 10, pp. 113299-113312, 2022, doi: 10.1109/ACCESS.2022.3218328.
[32] U. Cali et al., "A comprehensive academic and industrial survey of blockchain technology for the energy sector using fuzzy Einstein decision-making," Renewable and Sustainable Energy Reviews, vol. 211, 2025, doi: 10.1016/j.rser.2025.115845.
[33] O. Flor-Unda, F. Simbaña, X. Larriva-Novo, Á. Acuña, R. Tipán, and P. Acosta-Vargas, "A Comprehensive Analysis of the Worst Cybersecurity Vulnerabilities in Latin America," Informatics, vol. 10, no. 3, 2023, doi: 10.3390/informatics10030071.
[34] M. A. Juárez-Merino, "Digital governance in Latin America: A comprehensive analysis and future perspectives," Journal of Computational Social Science, 2025, doi: 10.1177/27723577251388360.