Panorama actual de la ciberseguridad: amenazas, legislación y brechas estructurales desde una revisión sistemática

Current cybersecurity landscape: threats, legislation, and structural gaps from a systematic review

Néstor Torres Gamarra
https://orcid.org/0009-0007-5406-5482
ntorresg@ucsm.edu.pe
Universidad Católica de Santa María
Arequipa-Perú

Manuel Zúñiga Carnero
https://orcid.org/0000-0002-1091-9438
mzuñigac@ucsm.edu.pe
Universidad Católica de Santa María
Arequipa-Perú

REVISTA INVECOM ISSN: 2739-0063

Recibido: 05-03-2025 Aceptado: 02-06-2025

2026. V6. N1.

Resumen

La ciberseguridad en el Perú representa un desafío estratégico creciente, impulsado por el aumento constante de ataques digitales, la rápida digitalización de los sectores productivos y las brechas normativas existentes. En este contexto, este estudio examina el panorama actual mediante una revisión sistemática de literatura científica publicada entre 2020 y 2024, con base en Scopus y un enfoque histórico-lógico. Para ello, se seleccionaron 24 estudios que abordan aspectos como los tipos de ciberataques más comunes, el nivel de madurez en ciberseguridad, la legislación vigente, la inversión empresarial, los avances tecnológicos y el mercado laboral especializado. Los hallazgos indican que el país enfrenta un alto volumen de ataques, principalmente *phishing* y fraude electrónico, que generan pérdidas económicas crecientes y limitan la capacidad de respuesta. Además, se evidenció que Perú se encuentra en una etapa inicial del Modelo de Madurez de Capacidades en Ciberseguridad (CMM), con una legislación desactualizada y baja coordinación institucional. Aunque la inversión en ciberseguridad ha aumentado, persiste una escasez crítica de talento especializado, lo que afecta la eficacia de las políticas de defensa digital. Por ello, es fundamental diseñar una estrategia nacional integral que fortalezca el marco normativo, impulse la formación técnica especializada y fomente la cooperación multisectorial. Solo así será posible enfrentar con resiliencia el complejo ecosistema de amenazas digitales que afecta al país.

Palabras clave: brecha digital, ciberseguridad, madurez institucional.

Abstract

Cybersecurity in Peru represents a growing strategic challenge, driven by the constant increase in digital attacks, the rapid digitalization of productive sectors, and existing regulatory gaps. In this context, this study examines the current landscape through a systematic review of scientific literature published between 2020 and 2024, based on Scopus and a historical-logical approach. To this end, 24 studies were selected that address aspects such as the most common types of cyberattacks, the level of cybersecurity maturity, current legislation, business investment, technological advances, and the specialized labor market. The findings indicate that the country faces a high volume of attacks, primarily phishing and electronic fraud, which generate growing economic losses and limit response capacity. Furthermore, it was evident that Peru is in an early stage of the Cybersecurity Capability Maturity Model (CMM), with outdated legislation and poor institutional coordination. Although investment in cybersecurity has increased, a critical shortage of specialized talent persists, affecting the effectiveness of digital defense policies. Therefore, it is essential to design a comprehensive national strategy that strengthens the regulatory framework, promotes specialized technical training, and fosters multisectoral cooperation. Only then will it be possible to resiliently confront the complex ecosystem of digital threats affecting the country.

Keywords: digital divide, cybersecurity, institutional maturity.

Introducción

La creciente digitalización de los procesos productivos, gubernamentales y sociales ha ampliado significativamente las superficies de exposición a riesgos cibernéticos, posicionando a la ciberseguridad como una prioridad estratégica a nivel global. En este sentido, Perú enfrenta desafíos importantes que amenazan su estabilidad digital, infraestructura crítica y soberanía tecnológica. Aunque se ha registrado una disminución en los intentos de ataque —de 15 mil millones en 2022 a 5 mil millones en 2023—, las pérdidas económicas asociadas a delitos informáticos alcanzaron los S/ 40 millones (BCRP, 2024; Forbes, 2024), lo que evidencia que la sofisticación de las amenazas supera los avances defensivos implementados.

Asimismo, el país se encuentra aún en la etapa formativa del Modelo de Madurez de Capacidades en Ciberseguridad (CMM), ubicándose por debajo del estándar regional (Martín, 2023). Esta situación se agrava debido a una legislación desactualizada y poco alineada con los riesgos emergentes del entorno digital. Aunque existen normas como la Ley de Protección de Datos Personales (Ley N.º 29733) y la Ley de Delitos Informáticos (Ley N.º 30096), ambas han quedado rezagadas frente a la velocidad de innovación de las amenazas (Congreso de la República, 2021; 2023). Además, la limitada implementación de la Política Nacional de Ciberseguridad, aprobada en 2017, dificulta la articulación efectiva entre los sectores público, privado y académico (Presidencia del Consejo de Ministros, 2017).

Por otro lado, la brecha de talento especializado en el ámbito laboral es alarmante. La demanda de profesionales en tecnologías de la información, ciberseguridad e inteligencia artificial ha crecido entre un 50 % y 60 % en los últimos tres años (ProInnóvate, 2024), pero la oferta sigue siendo insuficiente para cubrir las necesidades de empresas, entidades públicas y plataformas digitales en expansión. Esta carencia genera vacantes sin cubrir, sobrecarga de equipos y mayor vulnerabilidad frente a ataques dirigidos (OEA, 2023; Towhidi, 2023). Sectores como transporte, salud y logística se han visto especialmente comprometidos debido a su alta dependencia de sistemas interconectados (Bermúdez & Cano, 2023; Cervera & Alyson, 2024).

Simultáneamente, la adopción de tecnologías emergentes —como el Internet de las cosas (IoT), la computación en la nube y los sistemas de inteligencia artificial— presenta tanto oportunidades como riesgos. Estudios recientes advierten que, sin una gobernanza adecuada y mecanismos de protección efectivos, estas tecnologías amplían los vectores de ataque y aumentan la exposición a incidentes de seguridad (Ortiz, 2023; Reyes, 2023). Por ello, la gestión de estos desafíos requiere marcos regulatorios más flexibles, mayor inversión en infraestructura y mecanismos de control, así como la formación continua del capital humano. Aunque la inversión en ciberseguridad en Perú ha crecido de un 3 % a un 10 % en los últimos años (Calderón, 2020), sigue siendo insuficiente frente a los costos promedio por ataque, que pueden oscilar entre 13 mil y más de 5 millones de dólares (Gómez, 2023).

Este panorama se inscribe en una realidad regional marcada por asimetrías normativas y debilidades estructurales. En comparación con países como Estados Unidos o Canadá, que han consolidado políticas activas de diplomacia cibernética y alianzas estratégicas (Aguilar, 2024), Perú depende aún en gran medida de proveedores internacionales y carece de un modelo robusto de ciberdefensa nacional (Amasifuen, 2024). Por lo

tanto, resulta urgente adoptar un enfoque holístico e intersectorial que fortalezca las capacidades locales, promueva la innovación regulatoria, incentive la cooperación multinivel y articule esfuerzos sostenibles de alfabetización digital.

En este marco, el presente estudio tiene como propósito analizar el estado actual de la ciberseguridad en el Perú, considerando los tipos de ataques más frecuentes, los costos asociados, el nivel de madurez institucional, la legislación vigente, las tendencias tecnológicas y la dinámica del mercado laboral. Para ello, se emplea una revisión sistemática de literatura académica y técnica publicada entre 2020 y 2024, seleccionada en la base de datos Scopus. Se espera que los hallazgos contribuyan a identificar las principales brechas estructurales del país y a proponer lineamientos estratégicos que refuercen su resiliencia cibernética en un entorno global cada vez más complejo y hostil.

Metodología

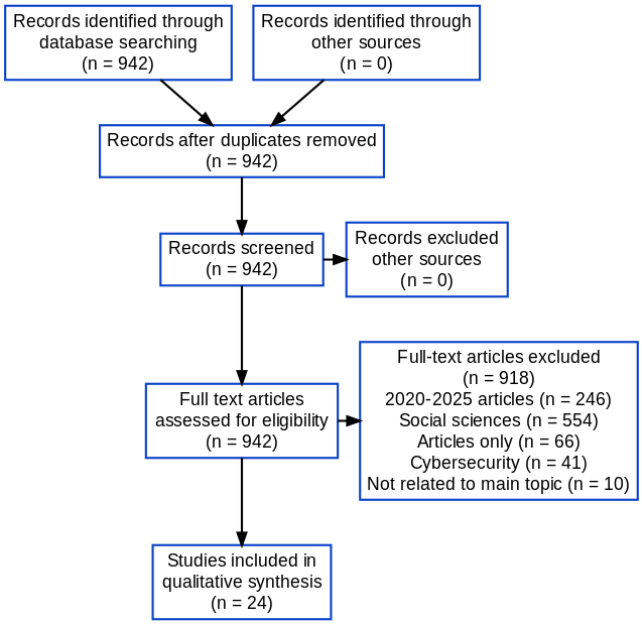
El presente estudio adoptó un enfoque metodológico basado en una revisión sistemática de la literatura, con el propósito de examinar rigurosamente el estado actual de la ciberseguridad en el Perú entre 2010 y 2024. Para ello, se utilizó el método histórico-lógico como marco analítico, lo que permitió rastrear la evolución de políticas, prácticas, tendencias y desafíos relacionados con la seguridad digital en el contexto nacional.

En este proceso, la estrategia de búsqueda bibliográfica se llevó a cabo en bases de datos científicas de alto impacto, como Scopus, seleccionadas por su solidez académica y relevancia temática. Asimismo, la ecuación de búsqueda fue diseñada para maximizar la relevancia y precisión de los resultados, combinando operadores booleanos y términos clave vinculados a la ciberseguridad, tales como: (*TITLE-ABS-KEY* ("*cybersecurity*" *OR* "*information security*" *OR* "*cyber resilience*" *OR* "*digital resilience*" *OR* "*resilience*")) *AND* (*TITLE-ABS-KEY* ("*cyber attacks*" *OR* "*cyber threats*" *OR* "*security incidents*" *OR* "*data breaches*" *OR* "*malware*" *OR* "*phishing*" *OR* "*ransomware*")) *AND* (*TITLE-ABS-KEY* ("*policy*" *OR* "*regulation*" *OR* "*law*" *OR* "*governance*" *OR* "*legal framework*" *OR* "*compliance*" *OR* "*normative framework*")) *AND* (*TITLE-ABS-KEY* ("*capacity building*" *OR* "*training*" *OR* "*skills development*" *OR* "*capabilities*" *OR* "*education*" *OR* "*awareness*")).

Esta búsqueda avanzada, aplicada en los campos de título, resumen y palabras clave (*TITLE-ABS-KEY*), permitió identificar artículos relevantes y actualizados que abordan aspectos técnicos, normativos y formativos de la ciberseguridad. Además, la ecuación fue refinada de manera iterativa para evitar resultados irrelevantes y garantizar una cobertura adecuada del fenómeno desde una perspectiva multidimensional.

Figura 1

Diagrama de flujo PRISMA mostrando el proceso de selección de artículos



Nota. Contenido generado desde https://hollyhartman.shinyapps.io/PRISMAFlowDiagram/

El proceso inicial de identificación arrojó un total de 942 registros tras eliminar duplicados, sin encontrarse fuentes adicionales mediante otros medios. A continuación, todos los registros fueron sometidos a un riguroso proceso de cribado, en el que se evaluaron los títulos, resúmenes y palabras clave, conservando únicamente aquellos que se alineaban con los objetivos del estudio. Para ello, se aplicaron criterios de inclusión claramente definidos: se consideraron exclusivamente estudios en español e inglés, publicados entre 2010 y 2024, que abordaran explícitamente temas relacionados con ciberseguridad, ciberataques, legislación, costos, tendencias tecnológicas o dinámica del mercado laboral.

Posteriormente, se procedió a la evaluación de los textos completos de los 942 artículos para determinar su elegibilidad. De este conjunto, se excluyeron 918 estudios por diversas razones: 246 no cumplían con el rango temporal establecido (2020–2025), 554 pertenecían al campo de las ciencias sociales sin conexión directa con la temática de ciberseguridad, 66 eran artículos incompletos o no revisados por pares, 41 carecían de contribuciones sustantivas al tema específico, y 10 no guardaban relación alguna con el eje central del estudio. Como resultado de este proceso sistemático de selección, se incluyeron 24 estudios en la síntesis cualitativa final.

La extracción y organización de datos se realizó mediante técnicas de análisis temático y síntesis narrativa. Se examinaron en detalle las dimensiones abordadas por cada estudio, incluyendo tipos de ciberataques, marcos legales vigentes, niveles de madurez institucional, patrones de inversión, avances en tecnologías emergentes y brechas en el mercado laboral. Esta sistematización permitió construir una visión comprensiva, crítica y contextualizada sobre los desafíos y oportunidades que enfrenta el Perú en materia de ciberseguridad, sentando las bases para futuras investigaciones y recomendaciones estratégicas.

Resultados

A medida que el entorno digital gana protagonismo en todos los sectores productivos, la ciberseguridad se ha consolidado como un eje estratégico fundamental dentro de las políticas públicas y el desarrollo empresarial en el Perú. Sin embargo, diversos informes señalan que durante 2023 el país fue blanco de más de 5 mil millones de intentos de ciberataques, una cifra alarmante que refleja tanto la creciente sofisticación de las amenazas como la urgente necesidad de fortalecer los sistemas de protección (Forbes, 2024; PNP, 2024). Según el Informe del BCRP (2024), las pérdidas económicas derivadas de estos delitos informáticos alcanzan cifras multimillonarias, afectando a empresas que pueden perder desde US$ 13 mil hasta más de US$ 5 millones por incidente, como advierte Gómez (2023).

No obstante, a pesar de estos indicadores preocupantes, persisten rezagos normativos y técnicos en la implementación de una política nacional integral de ciberseguridad (Presidencia del Consejo de Ministros, 2017; Amasifuen, 2024), lo que contrasta con los avances observados en países vecinos o aliados estratégicos como Estados Unidos y Canadá (Aguilar, 2024).

El panorama global evidencia una necesidad urgente de cooperación multilateral y armonización normativa en materia de ciberseguridad. En Norteamérica, por ejemplo, se ha consolidado un ecosistema regulatorio más cohesionado que facilita la interoperabilidad de sistemas y el intercambio de inteligencia frente a amenazas emergentes (Aguilar, 2024). Mientras tanto, en el Perú, el marco legal se ha ido fortaleciendo de forma fragmentada, con normativas como la Ley de Protección de Datos Personales (Congreso de la República, 2021) y la Ley de Delitos Informáticos (Congreso de la República, 2023), las cuales, si bien representan avances, no se articulan de manera suficiente con los desafíos que impone el actual entorno digital. Como destacan Bravo (2024) y Martín (2023), el país aún depende de una respuesta mayoritariamente reactiva ante los ataques cibernéticos, situación que también ha sido documentada por Optiv (2019) al señalar que muchas empresas están atrapadas en un ciclo de respuesta y no de prevención. Esta falta de anticipación se agrava por la escasa inversión sostenida en tecnología, infraestructura y talento humano especializado (Calderón, 2020; ProInnóvate, 2024).

Frente a este contexto, diversas investigaciones coinciden en la urgencia de transitar hacia modelos proactivos y adaptativos de gestión del riesgo digital. El uso de plataformas de protección de puntos finales, como las descritas por Evgeny et al. (2023), junto con la implementación de marcos de gobernanza tecnológica en sectores estratégicos como salud (Cervera & Alyson, 2024), transporte (Bermúdez & Cano, 2023) y educación superior (Towhidi, 2023), se perfilan como componentes esenciales en una estrategia nacional coherente. Además, el desarrollo de capacidades en aprendizaje automático para la detección de amenazas (Reyes et al., 2023) y el análisis de arquitecturas IoT (Ausecha et al., 2022) abren nuevas posibilidades para fortalecer la resiliencia digital. La OEA (2023) advierte sobre el déficit de profesionales capacitados en ciberseguridad en la región, lo que exige un compromiso interinstitucional para la formación de talento, mientras autores como Sánchez (2022) y Tapia (2021) enfatizan que el fenómeno debe abordarse también desde una perspectiva sociocultural y

de derechos. Así, la ciberseguridad no solo implica una mejora tecnológica, sino una transformación estructural, ética y educativa que garantice una ciudadanía digital protegida y consciente.

Perú se ha consolidado como uno de los principales objetivos de ciberataques en América Latina. Aunque el número de intentos de intrusión ha disminuido en comparación con el año anterior, la cantidad sigue siendo alarmante y continúa generando pérdidas económicas significativas. En este contexto, modalidades como el *phishing*, el fraude electrónico y el robo de identidad —que en conjunto representan más del 80 % de los delitos cibernéticos de índole económica— ponen de manifiesto la sofisticación y frecuencia de estas amenazas.

Esta situación se agrava debido a las debilidades estructurales del ecosistema digital peruano, entre las que destacan brechas legislativas, infraestructuras tecnológicas obsoletas y una limitada capacidad de respuesta frente a ataques dirigidos a sectores críticos como el transporte, la salud y la logística. En efecto, el país aún se encuentra en la etapa formativa del Modelo de Madurez de Capacidades en Ciberseguridad (CMM), lo que refleja una capacidad institucional restringida para enfrentar con eficacia los riesgos cibernéticos.

Además, esta condición no solo genera vulnerabilidades operativas, sino que también evidencia una desconexión entre la normativa vigente y la naturaleza dinámica del entorno digital. Si bien se han promulgado leyes clave relacionadas con la protección de datos y los delitos informáticos, su alcance resulta insuficiente ante la rápida evolución tecnológica y la aparición constante de nuevos vectores de ataque. Por otro lado, aunque la inversión empresarial en ciberseguridad ha mostrado un crecimiento progresivo, todavía no logra compensar las deficiencias en gobernanza digital ni cerrar la brecha de riesgo que amenaza la sostenibilidad de los sistemas críticos nacionales.

Uno de los desafíos más urgentes que enfrenta Perú es la escasez de talento especializado en ciberseguridad. A pesar de que la demanda de profesionales en esta área ha aumentado entre un 50 % y 60 % en los últimos años, las organizaciones continúan enfrentando dificultades significativas para cubrir vacantes estratégicas. Esta disparidad entre la oferta y la demanda genera una sobrecarga en los equipos técnicos y debilita la capacidad del país para implementar políticas preventivas efectivas.

Asimismo, factores como la digitalización acelerada, la proliferación del Internet de las Cosas (IoT) y la adopción masiva de servicios en la nube incrementan la complejidad de las amenazas, lo que exige contar con un cuerpo profesional altamente capacitado. Por lo tanto, sin una estrategia coordinada entre el gobierno, la academia y la industria para fortalecer el capital humano, Perú corre el riesgo de consolidar su vulnerabilidad estructural en un ecosistema digital que se vuelve cada vez más hostil.

Tabla 1

Sistematización de artículos sobre ciberseguridad

Autor y año	Temática	Hallazgos
Dumchikov et al. (2025)	Uso de inteligencia artificial en delitos cibernéticos	La IA representa un riesgo creciente en cibercrimen, pero también una herramienta útil para la investigación forense digital; se destaca la necesidad de marcos éticos y legales.
Mahyoub et al. (2025)	Ciberseguridad en el modelo de trabajo remoto (WFA)	Falta de formación en ciberseguridad y estrategias de comunicación en el modelo WFA; se proponen recomendaciones para mitigar riesgos cibernéticos.
Lukáč et al. (2025)	Factores socioeconómicos en la alfabetización digital y la seguridad	El nivel educativo y acceso a recursos están ligados a la capacidad de respuesta frente a amenazas digitales; se proponen programas educativos diferenciados.
Serini (2024)	Conciencia cibernética situacional en la Unión Europea	El intercambio de información de ciberseguridad enfrenta obstáculos legales; se requiere mayor cooperación institucional y resguardo de datos sensibles.
Chidukwani et al. (2024)	Ciberseguridad en pequeñas y medianas empresas (SMBs)	Falta de presupuesto y conocimiento limitan la ciberseguridad en las SMBs; Google es la fuente más usada, pero poco confiable para estas necesidades.
Zanke et al. (2024)	Cultura organizacional en seguridad de la información	Un enfoque mixto evidencia deficiencias en comunicación y formación sobre seguridad; se valida la utilidad de métodos cualitativos en diagnóstico organizacional.

Orosco-Fabian (2024)	Ciberseguridad en la educación superior	Aumento sostenido de estudios sobre ciberseguridad educativa desde 2003; temas centrales incluyen GDPR, amenazas cibernéticas y conciencia en ciberseguridad.
Ricci et al. (2024)	Brechas en la educación en ciberseguridad en Europa	La falta de conciencia social y de certificaciones a nivel UE limita la efectividad de la formación; se propone adaptar estrategias según cada país.
Koolen et al. (2024)	Medidas técnicas y organizativas según modelos de madurez en ciberseguridad	Se propone usar modelos de madurez para evaluar medidas de seguridad 'apropiadas' según el RGPD; se busca pasar de la comprensión técnica al cumplimiento legal.
Houichi et al. (2024)	Amenazas cibernéticas en ciudades inteligentes	Las *smart cities* enfrentan amenazas complejas debido a su dependencia tecnológica; se proponen contramedidas específicas por sectores como salud, movilidad y gobierno inteligente.
Nastjuk et al. (2024)	Entrenamiento en políticas de seguridad para empleados	El uso de argumentos de disuasión mejora la retención del aprendizaje y el cumplimiento de políticas de seguridad en empleados, con efectos sostenidos en el tiempo.
Song & Park (2024)	Simulación costo-beneficio para políticas de ciberresiliencia en PYMEs	Los incentivos fiscales son más efectivos que la regulación para fortalecer la ciber resiliencia en PYMEs; se propone un modelo dinámico con escenarios gubernamentales.
Dodge et al. (2023)	Motivación de usuarios para adoptar prácticas de ciberseguridad	El costo percibido, la autoeficacia y la severidad de las amenazas influyen en la intención de los usuarios para adoptar prácticas de ciberseguridad; se recomienda enfoque personalizado.
Rawindaran et al. (2023)	Ciberseguridad en PYMEs de Gales y relación con el gobierno	Las PYMEs colaboran con el gobierno para superar desafíos cibernéticos; el estudio resalta barreras financieras y falta de personal capacitado como retos centrales.
Tok & Chattopadhyay (2023)	Ciberdelito y oportunidades forenses en ciudades inteligentes	Se propone modelo de amenazas STRIDE para investigar delitos digitales en infraestructuras urbanas; destaca la necesidad de capacidades forenses y cooperación internacional.
Alsharida et al. (2023)	Conducta humana ante la ciberseguridad	Revisión sistemática muestra predominancia de teorías como PMT y TPB; se identifican brechas metodológicas y se enfatiza el rol de estudiantes y redes sociales en el estudio del comportamiento.
Smikle (2023)	Ciberseguridad en el sector financiero de Jamaica	La ciberseguridad es un asunto de política nacional; Jamaica requiere mayor capacidad para responder a ciberataques financieros y legislación específica.
Alhumud et al. (2023)	Evaluación del desempeño en ciberseguridad en universidades saudíes	Las universidades muestran cumplimiento parcial de normativas de ciberseguridad; se identifican debilidades en políticas, formación y monitoreo continuo.
Wong et al. (2022)	Conciencia de políticas de ciberseguridad y cumplimiento en empleados	La conciencia de políticas y la higiene cibernética del personal impactan en la capacidad de respuesta ante ciberataques en PYMEs; se resalta la importancia del enfoque preventivo.
Pravdiuk (2022)	Regulación legal de la ciberseguridad en Ucrania	La legislación ucraniana muestra avances y limitaciones en la protección del ciberespacio nacional; se enfatiza la necesidad de coordinación entre sectores público, privado y sociedad civil.
Mat et al. (2022)	Desafíos emergentes de ciberseguridad	Las medidas de ciber resiliencia en Malasia son limitadas por la falta de expertos, legislación fragmentada y escasa colaboración público-privada; se destaca la urgencia de mejorar la educación en ciberseguridad.

Zhang et al. (2022)	Amenazas desde información abierta en infraestructura crítica	El uso de OSINT permite a actores maliciosos acceder a datos sensibles de infraestructura crítica; se recomienda mayor control sobre la información pública y programas de concienciación.
Gibbs (2020)	Ciberseguridad económica en los Emiratos Árabes Unidos	A pesar del marco legal, el factor humano sigue siendo la mayor vulnerabilidad; la educación en ciberseguridad y la concienciación pública son claves para una cultura digital segura en la región.

Por último, el análisis de tendencias y proyecciones revela un cambio paradigmático en la manera en que las organizaciones enfrentan la ciberseguridad, destacando la incorporación de tecnologías emergentes como la inteligencia artificial y el Internet de las cosas. Estas innovaciones brindan importantes ventajas, especialmente en la detección automatizada de amenazas y en la capacidad de respuesta en tiempo real; no obstante, también amplían considerablemente la superficie de ataque.

Asimismo, continúan presentes desafíos estructurales, tales como la complejidad en la configuración de servicios en la nube, la falta de soberanía sobre los datos y la vulnerabilidad ante errores humanos. La combinación de estos factores pone de manifiesto que la transformación digital en el Perú no podrá sostenerse sin una política de ciberseguridad sólida, transversal y articulada, que reconozca tanto los riesgos tecnológicos como las debilidades humanas e institucionales.

Discusión

El análisis sistemático de 24 investigaciones recientes permite identificar tendencias clave en ciberseguridad desde diversas perspectivas: tecnológica, organizacional, legal y educativa. En primer lugar, uno de los hallazgos más relevantes es la dualidad de la inteligencia artificial en el ciberespacio. Por un lado, Dumchikov et al. (2025) y Tok & Chattopadhyay (2023) evidencian su uso tanto en actividades delictivas como en procesos de investigación forense; por otro lado, Houichi et al. (2024) y Zhang et al. (2022) advierten sobre su contribución al aumento de vulnerabilidades en ciudades inteligentes e infraestructuras críticas. En conjunto, estos estudios coinciden en que la adopción tecnológica debe ir acompañada de capacidades de defensa adaptativas y marcos éticos sólidos.

En segundo término, la ciberseguridad en pequeñas y medianas empresas (PYMEs) se presenta como un área especialmente vulnerable. Investigaciones como las de Chidukwani et al. (2024), Song & Park (2024), Rawindaran et al. (2023) y Wong et al. (2022) muestran que factores como el bajo presupuesto, la escasa formación y la falta de una cultura preventiva afectan negativamente su resiliencia digital. Frente a ello, las propuestas más efectivas giran en torno a incentivos fiscales, el fortalecimiento de la conciencia del personal y un rol activo del gobierno en la gestión de la respuesta post-incidente.

Por otra parte, en el ámbito educativo y organizacional se confirma la importancia de la formación y la cultura en ciberseguridad. Zanke et al. (2024), Nastjuk et al. (2024) y Dodge et al. (2023) destacan que las políticas de capacitación deben estar alineadas con los perfiles de los usuarios para lograr un impacto sostenido. Asimismo, Orosco-Fabian (2024), Alhumud et al. (2023) y Ricci et al. (2024) alertan sobre la carencia de estándares internacionales claros en la educación superior, mientras que Alsharida et al. (2023) subrayan la necesidad de adaptar las teorías conductuales a los nuevos contextos digitales.

En cuanto a los aspectos legales, los estudios de Serini (2024), Pravdiuk (2022), Smikle (2023), Mat et al. (2022) y Gibbs (2020) ponen de relieve la falta de articulación normativa y la necesidad de coherencia entre los marcos regulatorios nacionales e internacionales. En este sentido, Koolen et al. (2024) proponen modelos de madurez que traducen las obligaciones legales en acciones operativas sostenibles. Esta propuesta se complementa con la demanda de una mayor coordinación entre los sectores público y privado para garantizar una gobernanza digital robusta.

Finalmente, no puede subestimarse el papel de los factores individuales y contextuales en la ciberseguridad. Lukáč et al. (2025) y Dodge et al. (2023) demuestran que la alfabetización digital, la autoeficacia y la percepción de amenaza influyen directamente en la adopción de prácticas seguras. En conjunto, los estudios revisados indican que la ciberseguridad requiere una visión integral e intersectorial que articule tecnología, formación, normativa y motivación individual para afrontar los riesgos emergentes con eficacia y equidad.

Conclusiones

Los estudios revisados evidencian que la ciberseguridad es un fenómeno multidimensional que debe abordarse desde enfoques integrales e intersectoriales. En efecto, las amenazas digitales no se circunscriben

únicamente al ámbito tecnológico, sino que también impactan dimensiones legales, educativas, sociales y organizacionales. Por ello, resulta fundamental fortalecer los marcos normativos, fomentar la educación digital, promover culturas organizacionales resilientes y adaptar las estrategias a los diversos perfiles sociotécnicos para enfrentar los desafíos de un entorno digital en constante evolución.

De esta manera, se concluye que las políticas de ciberseguridad deben sustentarse en una visión articulada entre actores públicos y privados, en la que la formación continua, la concienciación del usuario final, la evaluación de riesgos y la aplicación contextualizada de tecnologías emergentes ocupen un lugar prioritario. En un mundo cada vez más interconectado, la construcción de capacidades cibernéticas sólidas e inclusivas no solo protege los activos digitales, sino que también garantiza la sostenibilidad, la confianza institucional y el desarrollo seguro de las sociedades.

Referencias

Aguilar, A. J. M. (2024). Rezago y asimetrías de las política nacional e internacional de ciberseguridad de México frente a Estados Unidos y Canadá: Retos de cooperación para Norteamérica. *Revista Académica del CISAN-UNAM, 19*(1), 38. https://dialnet.unirioja.es/descarga/articulo/9396821.pdf

Alhumud, T. A. A., Omar, A., & Altohami, W. M. A. (2023). An assessment of cybersecurity performance in the Saudi universities: A Total Quality Management approach. *Cogent Education, 10*(2), 2265227. https://doi.org/10.1080/2331186X.2023.2265227

Alsharida, R. A., Al-Rimy, B. A. S., Al-Emran, M., & Zainal, A. (2023). A systematic review of multi-prospects on human cybersecurity behavior. *Technology in Society, 73*, 102258. https://doi.org/10.1016/j.techsoc.2023.102258

Amasifuen, M. G. (2024). La ciberseguridad en el Perú. *El Peruano*.

BCRP. (2024). Informe anual sobre el impacto económico de los delitos cibernéticos en Perú (p. 58). https://www.bcrp.gob.pe/publicaciones/memoria-anual/memoria-2024.html

Bermúdez, C., & Cano, J. J. (2023). Cybersecurity model for the logistics and land transportation sectors. *Infosys, 8*. https://esdegrepositorio.edu.co/handle/20.500.14205/11147

Calderón, J. J. (2020). Crece inversión en seguridad tecnológica en empresas peruanas. *El Peruano*. https://elperuano.pe/noticia/89401-crece-inversion-en-seguridad-tecnologica-en-empresas-peruanas

Cervera, A., & Alyson, G. (2024). Cybersecurity and use of ICT in the health sector. *Atención Primaria, 56*(3). https://pubmed.ncbi.nlm.nih.gov/38219392/

Chidukwani, A., Zander, S., & Koutsakis, P. (2024). Cybersecurity preparedness of small-to-medium businesses: A Western Australia study with broader implications. *Computers & Security, 145*, 104026. https://doi.org/10.1016/j.cose.2024.104026

Congreso de la República del Perú (2021). Ley de Protección de Datos Personales peruana. *El Peruano*. https://www.leyes.congreso.gob.pe/documentos/leyes/29733.pdf

Congreso de la República del Perú (2023). Ley de Delitos Informáticos. *El Peruano*. https://www2.congreso.gob.pe/sicr/cendocbib/con5_uibd.nsf/C5F98BB564E5CCCF05258316006064AB/$FILE/6_Ley_30096.pdf

Dodge, C. E., Fisk, N., Burruss, G. W., Moule, R. K., & Jaynes, C. M. (2023). What motivates users to adopt cybersecurity practices? A survey experiment assessing protection motivation theory. *Criminology & Public Policy, 22*(4), 849–868. https://doi.org/10.1111/1745-9133.12641

Dumchikov, M., Maletova, O., Mishchenko, T., & Lytvynenko, Y. (2025). Artificial intelligence in cyberspace: Between danger and innovation. *Revista de Direito, Estado e Telecomunicacoes, 17*(1), 117–142. https://doi.org/10.26512/lstr.v17i1.53386

Forbes, S. (2024). El Perú sufrió 5.000 millones de intentos de ciberataques en 2023. *Forbes Perú*. https://forbes.pe/tecnologia/2024-03-25/el-peru-sufrio-5-000-millones-de-intentos-de-ciberataques-en-2023-reporto-fortinet/

Gibbs, T. (2020). Seeking economic cyber security: A Middle Eastern example. *Journal of Money Laundering Control, 23*(2), 493–507. https://www.emerald.com/insight/content/doi/10.1108/jmlc-09-2019-0076/full/html

Gomez, A. (2023). Ciberseguridad: Empresas pueden perder desde US$ 13 mil hasta más de US$ 5 millones por ataque. *El Peruano*. https://elcomercio.pe/tecnologia/ciberseguridad/ciberseguridad-empresas-pueden-perder-desde-us-13-mil-hasta-mas-de-us-5-millones-por-ataque-ciberdelincuencia-malware-phishing-suplantacion-de-identidad-noticia/

Houichi, M., Jaidi, F., & Bouhoula, A. (2024). A comprehensive and in-depth study of the threats faced by smart cities and the countermeasures implemented in their key areas. *Journal of Infrastructure, Policy and Development, 8*(10), 8629. https://systems.enpress-publisher.com/index.php/jipd/article/view/8629

ICEX España Exportación e Inversiones. (2023). Ficha sector: Ciberseguridad en Perú 2023. https://www.icex.es/es/quienes-somos/donde-estamos/red-exterior-de-comercio/PE/documentos-y-estadisticas/estudios-e-informes/visor-de-documentos.ficha-sector--ciberseguridad-en-per%C3%BA-2023.doc065202312

Koolen, C., Wuyts, K., Joosen, W., & Valcke, P. (2024). From insight to compliance: Appropriate technical and organisational security measures through the lens of cybersecurity maturity models. *Computer Law & Security Review, 52*, 105914. https://doi.org/10.1016/j.clsr.2023.105914

Lukáč, J., Kudlová, Z., Kopčáková, J., & Gallo, P. (2025). Impact of socio-economic factors on digital literacy and security. *TEM Journal, 14*(1), 925–932. https://www.temjournal.com/content/141/TEMJournalFebruary2025_925_932.pdf

Mahyoub, M., Matrawy, A., Isleem, K., & Ibitoye, O. (2025). Cybersecurity challenge analysis of work-from-anywhere (WFA) and recommendations guided by a user study. *IEEE Transactions on Human-Machine Systems*. https://arxiv.org/abs/2409.07567

Martín, M. V. (2023). Ciberseguridad en Perú. (O. E. Comercial, Ed.). *ICEX, 8*.

Mat, B., Pero, S. D. M., Zengeni, K. T., & Fakhrorazi, A. (2022). Towards an understanding of emerging cybersecurity challenges of a small state: A case study of Malaysia. *Tamkang Journal of International Affairs, 25*(3), 45–108. https://doi.org/10.6185/TJIA.V.202201_25(3).0002

Nastjuk, I., Rampold, F., Trang, S., & Benitez, J. (2024). A field experiment on ISP training designs for enhancing employee information security compliance. *European Journal of Information Systems*. https://doi.org/10.1080/0960085X.2024.2359460

OEA (2023). Fuerza laboral de ciberseguridad. Programa de Ciberseguridad del Comité Interamericano contra el Terrorismo. Organización de los Estados Americanos. https://www.oas.org/es/sms/cicte/docs/Reporte_sobre_el_desarrollo_de_la_fuerza_laboral_de_ciberseguridad_en_una_era_de_escasez_de_talento_y_habilidades.pdf

Optiv Security (2019). Empresas atrapadas en un ciclo de respuesta de ciberseguridad continuamente reactivo. *El Economista*. https://www.eleconomista.es/empresas-finanzas/noticias/9731425/02/19/Empresas-atrapadas-en-un-ciclo-de-respuesta-de-ciberseguridad-continuamente-reactivo-segun-un-informe-de-Optiv-Security.html

Orosco-Fabian, J. R. (2024). Cybersecurity in higher education: A bibliometric review. *Revista Digital de Investigación en Docencia Universitaria, 18*(2), e1933. http://www.scielo.org.pe/pdf/ridu/v18n2/2223-2516-ridu-18-02-e1933.pdf

Pravdiuk, A. (2022). The state and current issues of legal regulation of cyber security in Ukraine. *Evropsky Politicky a Pravni Diskurz, 9*(3), 19–28. http://repository.vsau.org/card.php?lang=en&id=31305

Presidencia del Consejo de Ministros (2017). Política Nacional de Ciberseguridad. *Diario El Peruano*. https://www2.congreso.gob.pe/sicr/cendocbib/con5_uibd.nsf/A36311FB344A1DC7052583160057706D/$FILE/Pol%C3%ADtica_Nacional_de_Ciberseguridad_peru.pdf

ProInnóvate (2024). Los perfiles profesionales tecnológicos más demandados en el Perú. Ministerio de la Producción. https://www.gob.pe/institucion/proinnovate/noticias/913473-los-perfiles-profesionales-tecnologicos-mas-demandados-en-el-peru-desarrolladores-ia-y-ciberseguridad-lideran-la-lista

Rawindaran, N., Jayal, A., Prakash, E., & Hewage, C. (2023). Perspective of small and medium enterprise (SMEs) and their relationship with government in overcoming cybersecurity challenges and barriers in Wales. *International Journal of Information Management Data Insights, 3*(2), 100191. https://doi.org/10.1016/j.jjimei.2023.100191

Reyes, E. (2023). Técnicas de aprendizaje automático para la detección y prevención de amenazas de ciberseguridad. Proyecciones futuras. *Revista Cubana de Ciencias Informáticas, 17*, 15–27. https://rcci.uci.cu/index.php/RCCI

Ricci, S., Parker, S., Jerabek, J., Lendak, I., & Janout, V. (2024). Understanding cybersecurity education gaps in Europe. *IEEE Transactions on Education, 67*(2), 190–201. https://ieeexplore.ieee.org/document/10380620

Sánchez, F. M. (2022). La seguridad en el ciberespacio desde una perspectiva sociocultural. *Revista de Ciencias Sociales, 2*, 243–258.

Serini, F. (2024). Collective cyber situational awareness in EU. A political project of difficult legal realisation? *Computer Law & Security Review, 55*, 106055. https://doi.org/10.1016/j.clsr.2024.106055

Smikle, L. (2023). The impact of cybersecurity on the financial sector in Jamaica. *Journal of Financial Crime, 30*(1), 86–96. https://ideas.repec.org/a/eme/jfcpps/jfc-12-2021-0259.html

Song, J., & Park, M. J. (2024). A system dynamics approach for cost-benefit simulation in designing policies to enhance the cybersecurity resilience of small and medium-sized enterprises. *Information Development*. https://doi.org/10.1177/02666669241252996

Tapia, E., & Canizales, R. (2021). La importancia de la ciberseguridad y los derechos. *Misión Jurídica, 14*(20), 142–158. https://www.revistamisionjuridica.com/wp-content/uploads/2021/06/08-20-La-importancia-de-la-ciberseguridad-y-los-derechos-humanos-en-el-entorno-virtual.pdf

Tok, Y. C., & Chattopadhyay, S. (2023). Identifying threats, cybercrime and digital forensic opportunities in smart city infrastructure via threat modeling. *Forensic Science International: Digital Investigation, 45*, 301540. https://doi.org/10.1016/j.fsidi.2023.301540

Towhidi, G. P. J. (2023). Aligning cybersecurity in higher education with industry. *Journal of Information Systems Education, 34*(1), 70–83. https://jise.org/Volume34/n1/JISE2023v34n1pp70-83.pdf

Wong, L.-W., Lee, V.-H., Tan, G. W.-H., Ooi, K.-B., & Sohal, A. (2022). The role of cybersecurity and policy awareness in shifting employee compliance attitudes: Building supply chain capabilities. *International Journal of Information Management, 66*, 102520. https://doi.org/10.1016/j.ijinfomgt.2022.102520

Zanke, A., Weber, T., Dornheim, P., & Engel, M. (2024). Assessing information security culture: A mixed-methods approach to navigating challenges in international corporate IT departments. *Computers & Security, 144*, 103938. https://doi.org/10.1016/j.cose.2024.103938

Zhang, Y., Frank, R., Warkentin, N., & Zakimi, N. (2022). Accessible from the open web: A qualitative analysis of the available open-source information involving cyber security and critical infrastructure. *Journal of Cybersecurity, 8*(1), tyac003. https://doi.org/10.1093/cybsec/tyac003