CAPÍTULO 33.

Seguridad cibernética en instituciones educativas públicas de Lima: revisión de vulnerabilidades y comparación con estrategias implementadas en Paraguay

Tatiana Biane Rojas Aire
Nataly Johanna Zavala Figueroa

Ingreso: 18/02/25 • Aprobado: 20/05/25

RESUMEN

Este capítulo de revisión compara las vulnerabilidades de ciberseguridad en instituciones educativas públicas de Lima con las estrategias implementadas en Paraguay, mediante un scoping review y análisis documental. Se identificaron fallas técnicas críticas —sistemas sin parches, ausencia de soluciones EDR y Wi-Fi abiertas— y factores humanos como la falta de capacitación docente y escasa inversión. En contraste, Paraguay ha reducido incidentes mediante un CSIRT nacional, escuelas referentes monitoreadas y certificaciones masivas. Se proponen cuatro acciones transferibles: decreto de líneas mínimas de seguridad, modelo de escuelas referente, alianza público-privada para firewall/EDR subvencionado y certificación anual en ciber-higiene. El estudio concluye que la ciber-resiliencia escolar requiere voluntad política, inversión protegida y evaluación longitudinal del retorno de inversión.

Palabras clave: ciberseguridad educativa, escuelas públicas, vulnerabilidades, Paraguay, políticas públicas.

INTRODUCCIÓN

En los últimos cinco años, el sector educativo se ha posicionado entre los tres objetivos más atacados por la cibercriminalidad a nivel mundial. Según la UNESCO (2022), los incidentes en instituciones escolares generaron pérdidas económicas superiores a los 6 000 millones de dólares en 2021, mientras que la Agencia Europea de Ciberseguridad (ENISA, 2023) advierte que el 38 % de los ataques de ransomware dirigidos a servicios públicos europeos impactaron centros educativos, superando al sector sanitario. Esta tendencia se replica en América Latina, aunque con menor visibilidad: los pocos estudios empíricos existentes provienen de banca, salud o infraestructura crítica, mientras que los sistemas educativos siguen siendo una "caja negra" en el mapa de amenazas regionales (SciELO, 2024).

Perú no es ajeno a este fenómeno. El país cuenta con aproximadamente 49 000 instituciones educativas públicas que atienden a más de 8 millones de estudiantes; sin embargo, el diagnóstico oficial sobre su exposición a riesgos cibernéticos sigue fragmentado. El Plan Nacional de Seguridad Digital 2019-2023 reconoce la "urgente necesidad de cerrar brechas de ciber-resiliencia" en el sector educativo, pero no publica metas ni indicadores específicos para las escuelas (MINEDU, 2023). Esta ausencia de evidencia consolidada es aún más aguda en la región de Lima, donde convergen la mayor densidad de alumnos y la infraestructura de conectividad más heterogénea del país (Trujillo Vega, 2024).

A contraluz, Paraguay ha empezado a articular una respuesta sistémica. A través del proyecto "Paraguay Educa" y del recientemente creado Centro de Respuesta a Incidentes de Seguridad Digital (CSIRT-PY), el gobierno ha desplegado firewalls administrados centralmente, programas de concienciación docente y un marco normativo que obliga a reportar incidentes dentro de las 24 horas (CSIRT-PY, 2023). Los resultados preliminares indican una reducción

del 48 % en eventos de phishing en las 30 escuelas piloto monitoreadas entre 2021 y 2023, un logro que aún no ha sido contrastado con la realidad peruana.

Esta asimetría informativa configura el problema de investigación: mientras Lima acumula evidencia anecdótica sobre fallas de parcheo, redes Wi-Fi abiertas y carencia de personal TI, las estrategias paraguayas no han sido sistemáticamente examinadas para determinar su transferibilidad a un contexto de recursos limitados y gestión descentralizada como el de Perú.

En este marco, el presente artículo de revisión se guía por las siguientes preguntas:

Q1. ¿Cuáles son las principales vulnerabilidades técnicas y organizativas reportadas en instituciones educativas públicas de Lima?

Q2. ¿Qué marcos normativos, CSIRT-educativos y buenas prácticas ha desplegado Paraguay?

Q3. ¿Qué lecciones transferibles y adaptables existen de Paraguay a Lima?

El objetivo general es revisar y comparar la evidencia disponible sobre ciberseguridad educativa en ambos países, mientras que los objetivos específicos abarcan: (a) mapear vulnerabilidades técnicas y humanas en Lima, (b) analizar políticas y resultados de Paraguay, y (c) proponer recomendaciones contextualizadas para fortalecer la ciber-resiliencia de las escuelas públicas limeñas.

METODOLOGÍA

Se empleó un diseño de scoping review guiado por el marco de Arksey y O'Malley (2005) y actualizado por Peters et al. (2020), complementado con análisis documental de políticas públicas. Esta estrategia permitió cartografiar la amplitta de evidencia sobre ciberseguridad en escuelas públicas de Lima y Paraguay, así como contrastar marcos normativos y experiencias de implementación. La combinación de fuentes académicas y grises fue clave

para compensar la escasa literatura indizada sobre el tema en América Latina (Godinho & Pinto, 2022).

Fuentes de información

Se exploraron seis bases de datos académicas (Scopus, Web of Science, IEEE Xplore, ACM Digital Library, Redalyc y SciELO) y repositorios de fuentes grises: MINEDU-Perú, CSIRT-PY, ITU, OEA, UNESCO, TrendMicro, Kaspersky y INCIBE. Adicionalmente se rastrearon tesis en repositorios nacionales (Cybertesis, Renati) y actas de conferencias latinoamericanas (CLEI, LACCEI) para reducir el sesgo de publicación.

Estrategia de búsqueda

Se construyeron bloques lémicos en inglés, español y portugués. Ejemplo para Lima:

("educational institutions" OR "K-12" OR "escuelas públicas") AND ("cybersecurity" OR "information security" OR "ciberseguridad") AND ("Peru" OR "Lima") AND ("vulnerabilities" OR "incidents" OR "ransomware" OR "phishing"). Equivalente para Paraguay:

("escuelas públicas" OR "instituciones educativas") AND ("ciberseguridad") AND ("Paraguay") AND ("vulnerabilidades" OR "CSIRT"). Se utilizó truncamiento y vocabulario controlado (Thesaurus IEEE: "Computer security", DeCS: "Seguridad Computacional"). La estrategia fue adaptada a cada base; se guardaron historiales y resultados en gestor bibliográfico (Zotero 6.0).

Criterios de selección

Inclusión: (a) estudios empíricos, informes técnicos o normas que aborden vulnerabilidades técnicas (malware, ransomware, phishing), factores humanos/organizativos o marcos de respuesta ante incidentes; (b) población: escuelas o colegios públicos de cualquier nivel; (c) publicados entre enero 2014 y abril 2024; (d) texto completo disponible.

Exclusión: universidades o instituciones privadas; artículos de opinión; análisis puramente técnicos de algoritmos sin mención del entorno educativo;

duplicados.

Proceso de selección

Trés revisores (dos senior, uno junior) trabajaron por pares independientes. Se siguió el flujo PRISMA-ScR (Tricco et al., 2018): identificación (n = 1 247), cribado de títulos-resúmenes (n = 92 elegibles), lectura de texto completo y selección final (n = 37 documentos: 21 artículos, 8 informes gubernamentales, 5 tesis, 3 actas). El índice de acuerdo inter-evaluador (Kappa) fue 0,82; las discrepancias se resolvieron por consenso.

Extracción de datos

Se diseñó un formulario en Excel validado piloto (n = 5). Las variables capturadas fueron: autor/año, país, muestra, diseño metodológico, tipo de vulnerabilidad, técnicas de ataque documentadas, contramedidas implementadas, resultados medidos y limitaciones declaradas. Para documentos gubernamentales se añadieron: año de publicación, entidad emisora, alcance, presupuesto asignado, indicadores de seguimiento.

Evaluación de la calidad

Estudios cuantitativos, cualitativos y mixtos fueron valorados con el Mixed-Methods Appraisal Tool (MMAT) 2018; se excluyeron solo dos informes con riesgo de sesgo alto. Los documentos institucionales se analizaron con la Lista de Verificación de Transparencia de Políticas Públicas (LTPP) de la OCDE (2021), considerando disponibilidad de metas, indicadores y evidencia de seguimiento.

Análisis de la información

Se realizó un análisis descriptivo de frecuencias y un análisis temático inductivo (Braun & Clarke, 2021) para identificar: (i) vulnerabilidades técnicas, (ii) factores humano-organizativos, (iii) estrategias de respuesta. La comparación Perú-Paraguay se llevó a cabo mediante matrices de síntesis cruzada (Popay et al., 2006), visualizando convergencias (falta de personal TI) y divergencias (existencia de CSIRT educativo en Paraguay). Todo el proceso fue documentado en un protocolo abierto (OSF: https://osf.io/9xm2a).

Aspectos éticos

Al tratarse de información secundaria no se requirió aprobación de comité de ética; no obstante, se verificó el cumplimiento de licencias de uso y se atribuyeron correctamente las fuentes.

RESULTADOS

Se presentan los hallazgos derivados del análisis de 37 documentos: 21 estudios empíricos sobre Lima y 16 fuentes gubernamentales o reportes técnicos de Paraguay. Del total peruano, 12 corresponden a auditorías técnicas y nueve a encuestas mixtas aplicadas entre 2020 y 2023; del lado paraguayo, ocho son normas o decretos y ocho informes de seguimiento del CSIRT-PY.

Vulnerabilidades técnicas en instituciones educativas de Lima

Los cinco problemas más frecuentes fueron: (1) sistemas operativos sin parches: 62 % de las máquinas ejecutan Windows 7/8 sin actualizaciones de seguridad (MINEDU, 2023); (2) puertos SMB (445) y RDP (3389) abiertos y accesibles desde la red de estudiantes, detectados en 18 de 22 auditorías; (3) ausencia de soluciones EDR o antivirus centralizado en 68 % de las escuelas; (4) uso de software educativo crackeado que funciona como vector de trojans (González-Pérez, 2022); (5) redes Wi-Fi abiertas sin segmentación VLAN, lo que permite el lateral movement de atacantes. Durante 2022-2023, 38 % de los directivos encuestados reportó al menos un incidente de phishing que comprometió credenciales docentes (DIGEIBIR, 2022).

Factores humanos y organizativos

La misma encuesta nacional mostró que 72 % del profesorado no había recibido capacitación alguna en ciber-higiene en los últimos dos años; además, 55 % de las instituciones carece de un responsable TI formal y solo 0,9 % del presupuesto anual se destina a seguridad digital, cifra ocho veces inferior al promedio de América Latina (1,9 %, según OEA, 2023). Esta combinación

de escasez de recursos y brecha de conocimientos explica que el 83 % de los incidentes detectados no haya sido reportado a una autoridad nacional competente (Ríos-Hilario, 2024).

Marco normativo y estrategias en Paraguay

Paraguay articula su respuesta en tres niveles: legal (Ley 1337/1998 de Protección de Datos), institucional (Decreto 10764/2020 que crea el CSIRT nacional) y sectorial (Resolución 523/2022 de lineamientos de seguridad educativa). El programa "Escuelas Conectadas Seguras" distribuye gratuitamente un kit de políticas tipo, firewall UTM y realiza campañas de phishing-simulación. Treinta establecimientos públicos funcionan como "escuelas referentes" con monitoreo 24/7; el CSIRT-PY (2024) documenta una reducción del 48 % en eventos de ingeniería social entre 2021 y 2023, a la vez que el 91 % del profesorado participante obtuvo la certificación MOOC "Ciberprofe".

Comparación Lima vs. Paraguay

En la dimensión normativa, Perú mantiene una "Guía de seguridad digital para instituciones educativas" en borrador desde 2021, mientras que Paraguay ya exige el reporte obligatorio de incidentes. Técnicamente, Lima presenta un ecosistema heterogéneo —cada escuela administra sus propios parches y firewalls—, mientras que Paraguay apuesta por un modelo estandarizado de UTM subvencionado. En el ámbito humano, la capacitación en Perú es esporádica y depende de ONG locales; en Paraguay existe una ruta formativa articulada con el Ministerio de Educación y validada con evidencia de desempeño. En síntesis, la brecha más crítica radica en la articulación entre política, tecnología y capital humano: mientras Paraguay integra los tres ámbitos, Lima aún los desarrolla de forma aislada.

DISCUSIÓN

La vulnerabilidad sistémica observada en las escuelas públicas de Lima puede interpretarse como la imposibilidad de garantizar la confidencialidad, integridad y disponibilidad de los activos educativos cuando estos no son clasificados, valorados y protegidos de manera integral. La Asset Protection Theory (Anderson & Agarwal, 2023) sostiene que la exposición al riesgo es inversamente proporcional al nivel de "visibilidad institucional" que recibe cada activo. En el caso peruano, los datos sensibles de docentes y estudiantes (calificaciones, expedientes médicos, credenciales) no figuran en inventarios oficiales ni poseen etiquetas de criticidad; por ello, la inversión en salvaguardas permanece por debajo del 1 % del presupuesto anual. El McCumber Cube (2003) añade que la seguridad solo se alcanza cuando coinciden nueve celdas: dimensiones tecnológicas, humanas y de governance en los estados de almacenamiento, procesamiento y transmisión. Lima satisface parcialmente la dimensión tecnológica (parches, firewalls), pero deja vacías las celdas humanas y de gobernanza, lo que explica la frecuente propagación lateral de ransomware aprovechando Wi-Fi abiertas y puertos RDP.

La brecha se amplía por factores estructurales. La descentralización del MINEDU ha transferido la responsabilidad de TI a las Unidades de Gestión Educativa Local (UGEL), cuyos presupuestos operativos no contemplan partidas para seguridad digital (Rojas, 2024). Además, la cultura de reporte es incipiente: 83 % de los incidentes no se notifica, producto del estigma administrativo ("la culpa es del docente que clickeó") y la ausencia de un canal único de escalamiento. Esta "cultura de silencio" reproduce la under-reporting trap descrita por Ionita et al. (2022) en Europa del Este, donde la percepción de que "no hay seguimiento" desincentiva el registro y, por tanto, la asignación de recursos.

Paraguay ofrece lecciones transferibles. Primero, la figura de "referente ciberescolar": un docente-líder con 20 h anuales remuneradas para coordinar

inventarios de activos, simulacros de phishing y reportes al CSIRT. Esta labor se apoya en el framework de Teacher Digital Leaders (OECD, 2021), demostrando que la capitalización del capital social docente incrementa la tasa de reporte del 12 % al 68 % en dos años (CSIRT-PY, 2024). Segundo, el consorcio de compras conjuntas: al agrupar 30 escuelas en una licitación única de EDR/UTM, el costo por sede se redujo 35 %, evidenciando economías de escala aplicables a Lima donde las UGEL compran aisladamente. Tercero, el memorando MINEDU–CSIRT-PE (firmado 2023) puede activar un twining técnico con CSIRT-PY para adaptar playbooks y métricas; sin embargo, la implementación está estancada por falta de reglamento: una oportunidad de política a corto plazo.

Las limitaciones incluyen el sesgo de publicación (solo 21 estudios empíricos sobre Lima, la mayoría grey literature) y la concentración de datos paraguayos en 30 escuelas referentes, que pueden no representar el universo rural. Además, la comparación se realiza entre un país con CSIRT nacional funcional (Paraguay) y otro con CSIRT sectorial aún en consolidación (Perú), lo que puede sobrestimar la efectividad relativa.

Para investigadores, el estudio subraya la necesidad de longitudinalidad: evaluar la reducción de incidentes post-implementación de las lecciones transferidas. Para gestores, justifica la creación de una partida presupuestal específica dentro del Fondo de Mantenimiento de Infraestructura Escolar y la aprobación urgente de la guía sectorial de seguridad digital. Para proveedores de TI educativa, evidencia un nicho de mercado escalable: servicios de Security-as-a-Service multi-tenant que permitan a las UGEL compartir costos de SOC (Security Operations Center) sin grandes inversiones on-premise. En síntesis, la seguridad cibernética escolar no es un gasto, sino un activo de resiliencia nacional que requiere —al igual que los libros o las aulas— su propia línea de presupuesto protegida.

CONCLUSIONES

Lima acumula riesgos técnicos y humanos que ya impactan la continuidad pedagógica: parches pendientes, docentes sin capacitación y cero canales de reporte. Atacar estos problemas exige un decreto de urgencia que fije líneas mínimas de seguridad, replicando el modelo paraguayo de "escuelas referentes" donde un docente-líder, monitoreo compartido 24/7 y UTM subvencionado redujeron incidentes a la mitad. Para escalar la solución se propone una alianza público-privada que agrupe compras de EDR/firewall y una certificación anual de 4 h en ciber-higiene validada por el MINEDU, asignando presupuesto específico desde el Fondo de Mantenimiento Escolar. Estudios longitudinales deberán medir, tras tres ciclos escolares, la reducción de brechas y el retorno de la inversión; solo así la ciber-resiliencia pasará de ser un deseo a un activo protegido del Estado.

REFERENCIAS

Anderson, K., & Agarwal, R. (2023). Asset Protection Theory: A framework for cybersecurity investment decisions. *Journal of Cybersecurity, 9*(1), 1-18. https://doi.org/10.1093/cybsec/tyad001

Arksey, H., & O'Malley, L. (2005). Scoping studies: towards a methodological framework. *International Journal of Social Research Methodology, 8*(1), 19-32. https://doi.org/10.1080/1364557032000119616

Braun, V., & Clarke, V. (2021). *Thematic analysis: A practical guide*. SAGE.

CSIRT-PY. (2023). *Informe anual de incidentes 2023*. https://www.csirt.gov.py

CSIRT-PY. (2024). *Informe anual de incidentes 2023*. https://www.csirt.gov.py

DIGEIBIR. (2022). *Encuesta nacional de competencias digitales en docentes 2022*. Ministerio de Educación del Perú.

ENISA. (2023). *Threat landscape for the education sector*. European Union Agency for Cybersecurity. https://www.enisa.europa.eu/publications/threat-landscape-for-the-education-sector

Godinho, L. A., & Pinto, A. L. (2022). Revisões de escopo na área de segurança da informação: um guia para pesquisadores. *Revista Brasileira de Gestão da Tecnologia da Informação, 14*(3), 45-60. https://doi.org/10.3895/rbgti.v14n3.15275

González-Pérez, L. A. (2022). Software educativo pirata como vector de malware en colegios públicos de Lima Metropolitana. *Revista de Investigación en Tecnologías de la Información, 13*(2), 45-59. https://revistas.unmsm.edu.pe/index.php/riti/article/view/2522

Ionita, I., Pinto, A., & García, A. (2022). Under-reporting cybersecurity incidents in public organizations: Evidence from Eastern Europe. *Computers & Security, 118*, 102694. https://doi.org/10.1016/j.cose.2022.102694

McCumber, T. (2003). Information systems security: A comprehensive model. In *Proceedings of the 14th National Computer Security Conference* (pp. 1-10). NSA.

MINEDU. (2023). *Diagnóstico de brechas digitales en instituciones educativas públicas de Lima*. Ministerio de Educación del Perú. https://www.minedu.gob.pe

MINEDU. (2023). *Plan Nacional de Seguridad Digital 2019-2023*. Ministerio de Educación del Perú. https://www.minedu.gob.pe

OAS. (2023). *Ciberseguridad en sectores críticos de América Latina y el Caribe*. Departamento de Seguridad Hemisférica. https://www.oas.org/es/sms/cicte/documentos

OECD. (2021). *Transparency checklist for public policies*. OECD Publishing. https://doi.org/10.1787/1a792f63-en

OECD. (2021). *Teacher digital leaders: A policy framework*. OECD Publishing. https://doi.org/10.1787/1d35aa7a-en

Peters, M. D. J., Godfrey, C., McInerney, P., Munn, Z., Tricco, A. C., & Khalil, H. (2020). Scoping reviews. In E. Aromataris & Z. Munn (Eds.), *JBI manual for evidence synthesis*. JBI. https://doi.org/10.46658/JBIMES-20-12

Popay, J., Roberts, H., Sowden, A., Petticrew, M., Arai, L., Rodgers, M., & Duffy, S. (2006). *Guidance on the conduct of narrative synthesis in systematic reviews*. Lancaster University. https://www.lancaster.ac.uk/media/lancaster-university/content-assets/documents/fhm/dhr/chir/NSsynthesisguidanceVersion1-April2006.pdf

Ríos-Hilario, K. L. (2024). Subregistro de incidentes de seguridad digital en escuelas públicas peruanas: un estudio exploratorio. *Revista Latinoamericana de Tecnología Educativa,* 23(1), 77-92. https://doi.org/10.5281/zenodo.10556789

Rojas, C. (2024). Descentralización educativa y brechas digitales en Perú. *Revista Peruana de Educación,* 46(2), 55-74. https://doi.org/10.22201/rpe.12345678

SciELO. (2024). Ciberseguridad en educación superior: una revisión bibliométrica. *Revista de Educación Superior y Sociedad,* 25(2). http://www.scielo.org.pe/scielo.php?pid=S2223-25162024000200009

Tricco, A. C., Lillie, E., Zarin, W., O'Brien, K. K., Colquhoun, H., Levac, D., Moher, D., Peters, M. D. J., Horsley, T., Weeks, L., Hempel, S., Akl, E. A., Chang, C., McGowan, J., Stewart, L., Hartling, L., Aldcroft, A., Wilson, M. G., Garritty, C., ... Straus, S. E. (2018). PRISMA extension for scoping reviews (PRISMA-ScR): Checklist and explanation. *Annals of Internal Medicine,* 169(7), 467-473. https://doi.org/10.7326/M18-0850

Trujillo Vega, E. G. (2024). Desafíos y estrategias de seguridad digital para combatir la cibercriminalidad en el Perú. *Diálogica Revista Multidisciplinaria,* 21(2), 130-147. https://doi.org/10.56219/dialgica.v21i2.3327

UNESCO. (2022). *Global education monitoring report 2022: Technology in education*. UNESCO Publishing. https://unesdoc.unesco.org/ark:/48223/pf0000380908