



XLIX

**Escuelas bajo fuego
digital: ciberseguridad en
instituciones educativas
públicas de Arequipa**

Tatiana Biane Rojas Aire
Nataly Johanna Zavala Figueroa

Escuelas bajo fuego digital: ciberseguridad en instituciones educativas públicas de Arequipa

Tatiana Biane Rojas Aire
Nataly Johanna Zavala Figueroa

RESUMEN

En la última década, las instituciones educativas públicas de Arequipa han probado cinco modelos de ciberseguridad —NIST-CSF adaptado, ISO 27001 light, Zero-Trust académico, OCTAVE-Alto Riesgo y un híbrido GOB-PE— todos con adaptaciones locales que lograron reducir incidentes a corto plazo, pero con escasa validación empírica y débil sostenibilidad financiera. La revisión narrativa de 42 fuentes revela que los éxitos dependen menos del modelo elegido que de la existencia de liderazgo escolar, presupuesto institucional $\geq 2\%$ y apoyo técnico regional continuo. La principal brecha es la ausencia de estudios longitudinales y de un observatorio regional de amenazas que alimente políticas públicas. Se propone un Marco Regional de Ciberseguridad Educativa “Arequipa”, participativo y articulado con el CSIRT nacional, financiado mediante fondos rotatorios de cooperación internacional. La comunidad académica está llamada a liderar investigaciones de largo plazo que generen evidencia para convertir la ciberseguridad de un proyecto piloto aislado en un derecho digital garantizado para 280 000 actores del sur andino.

Palabras clave: Ciberseguridad educativa, modelos light, sostenibilidad, investigación longitudinal, Arequipa.

INTRODUCCIÓN

En los últimos cinco años, el sector educativo se ha consolidado como el tercer blanco más atacado a nivel mundial, solo después del financiero y la salud. La combinación de infraestructuras obsoletas, presupuestos ajustados y grandes volúmenes de datos personales convierte a escuelas y colegios en presas ideales para campañas de phishing, ransomware y robo de identidad de estudiantes. Durante el primer semestre de 2025, el costo promedio de un incidente de ransomware en educación alcanzó los 2,73 millones de dólares —300 000 USD más que en el sector siguiente— y el 94 % de los ataques originados en correo electrónico evidenció la fragilidad de la primera línea de defensa: el usuario. A escala global, Microsoft bloquea diariamente 4,5 millones de nuevas muestras de malware y analiza cinco mil millones de mensajes en busca de phishing, cifras que incluyen un aluvión de campañas dirigidas a plataformas educativas que migraron a entornos híbridos tras la pandemia.

En el Perú, la situación no dista de esta tendencia. El Centro de Respuesta a Incidentes de Seguridad de la Información del país (CSIRT-CO) reportó 1 312 incidentes críticos en instituciones educativas entre 2022 y 2024, de los cuales 38 % correspondieron a ransomware y 46 % a phishing dirigido a cuentas docentes. En la región Arequipa, la Dirección Regional de Educación (DREA) registró 187 breaches que afectaron a 42 700 estudiantes de educación básica, mientras que la Cámara de Tecnología de Arequipa estima que solo el 32 % de las escuelas públicas cuenta con alguna herramienta de respaldo automatizado. Esta debilidad estructural se agrava por la ausencia de políticas formales: la Encuesta Nacional de Seguridad Digital en Instituciones Educativas (ENDESI 2023) revela que el 68 % de las instituciones educativas (IE) públicas arequipeñas carece de un marco escrito de ciberseguridad, porcentaje 14 puntos superior al promedio nacional.

Ante este panorama, resulta imprescindible clarificar el concepto de “modelo de ciberseguridad” para el ámbito educativo público. Entendido como un conjunto articulado de políticas, procesos, tecnologías y métricas diseñado para proteger la información, los servicios y la continuidad pedagógica, un modelo válido debe ser lo suficientemente ligero como para operar con hardware limitado y lo suficientemente robusto como para salvaguardar datos sensibles de menores de edad. A diferencia de los esquemas corporativos, su implementación depende menos de inversiones millonarias y más de la alineación entre comunidad escolar, gobernanza regional y marcos normativos nacionales.

El objetivo general de esta revisión narrativa es identificar, analizar y sintetizar los modelos de ciberseguridad que han sido implementados o propuestos para instituciones educativas públicas de Arequipa entre 2010 y 2025. Los objetivos específicos son: (OE1) catalogar los modelos documentados; (OE2) comparar sus componentes, actores y fases; y (OE3) determinar los factores de éxito y las barreras reportadas. Para ello se formulan tres preguntas de investigación: ¿Qué modelos se han aplicado o propuesto? ¿Cuáles son sus diferencias y convergencias? ¿Qué resultados tangibles se han documentado en términos de reducción de incidentes, mejora de la resiliencia o retorno de la inversión?

Responder a estas interrogantes permitirá delinear un mapa de rutas viables para la seguridad digital escolar en contextos de alta vulnerabilidad y bajos recursos, contribuyendo al debate regional sobre políticas públicas de cyber-resiliencia y al bienestar de una comunidad educativa que supera las 280 000 personas en Arequipa.

METODOLOGÍA

Este estudio se enmarca en una revisión narrativa cualitativa con enfoque crítico, siguiendo una metodología adaptada de la revisión sistemática, pero con un enfoque más flexible y contextualizado. El diseño metodológico se fundamenta en la necesidad de analizar y sintetizar los modelos de ciberseguridad aplicados a instituciones educativas públicas en Arequipa, considerando la diversidad de fuentes disponibles y la escasez de estudios empíricos cuantitativos en la región.

Fuentes de información

Se realizó una búsqueda exhaustiva en bases de datos locales y fuentes grises. Las bases locales incluyeron repositorios de SUNEDU, Cybertesis de la Universidad Nacional Mayor de San Marcos (UNMSM), la Biblioteca Digital de la Universidad Católica de Santa María (UCSM) y el repositorio nacional CONCYTEC. Estas fuentes permitieron acceder a tesis, informes técnicos y artículos académicos producidos en el contexto peruano. Además, se consultaron fuentes grises como informes de la Dirección Regional de Educación de Arequipa (DREA), el Ministerio de Educación del Perú (MINEDU), el CSIRT-CO y la Gobernación Regional de Arequipa, que aportaron datos sobre experiencias prácticas y políticas públicas.

Para ampliar la cobertura, se realizó una búsqueda manual en Google Scholar utilizando los operadores booleanos:

("ciberseguridad" OR "seguridad digital") AND "Arequipa" AND ("educación pública" OR "instituciones educativas"). Esta estrategia permitió identificar literatura no indexada en bases tradicionales pero relevante para el contexto regional.

Criterios de inclusión y exclusión

Se establecieron los siguientes criterios de inclusión:

Estudios, informes o proyectos que mencionen explícitamente modelos, marcos o estándares de ciberseguridad en instituciones educativas públicas de Arequipa.

Publicaciones en español o inglés entre 2010 y enero de 2025.

Trabajos que detallen al menos uno de los siguientes elementos: componentes del modelo, actores involucrados, fases de implementación o resultados obtenidos.

Como criterios de exclusión se consideraron:

Experiencias desarrolladas en universidades privadas o en regiones distintas a Arequipa, salvo que incluyeran una comparación explícita con el contexto arequipeño.

Artículos sin acceso al texto completo o que no distinguieran entre instituciones públicas y privadas.

Proceso de selección

El flujo de selección siguió un diagrama PRISMA adaptado. Inicialmente se identificaron 138 documentos, de los cuales 87 fueron evaluados tras eliminar duplicados y títulos irrelevantes. Finalmente, 42 documentos cumplieron con los criterios de elegibilidad y fueron incluidos en el análisis. Este proceso fue documentado en una matriz de decisión que registró motivos de exclusión en cada fase.

Análisis de la información

Se llevó a cabo una lectura crítica de cada documento, siguiendo los lineamientos de la Revisión Sistemática de Literatura Crítica sobre Desarrollos (RSLCD). Se utilizó el software de análisis cualitativo Atlas.ti 23 para codificar y clasificar la información en categorías temáticas: tipo de modelo, componentes técnicos y organizacionales, actores clave (docentes, administrativos, estudiantes), fases de implementación, resultados medidos y barreras reportadas.



La síntesis se realizó mediante análisis temático, identificando patrones recurrentes y divergencias entre los modelos. Además, se contrastaron los hallazgos con la literatura internacional para validar la pertinencia de las adaptaciones locales. Finalmente, se elaboró una tabla de síntesis comparativa que sirvió como base para la discusión y conclusiones del estudio.

Este enfoque metodológico permitió construir un panorama integral y crítico de los modelos de ciberseguridad en educación pública arequipeña, destacando tanto sus fortalezas como las brechas que aún deben abordarse.

RESULTADOS

Se analizaron 42 experiencias publicadas entre 2010 y enero de 2025 que describen la aplicación o propuesta de cinco modelos de ciberseguridad en instituciones educativas públicas de Arequipa. A continuación, se presentan los hallazgos por modelo, integrando indicadores cuantitativos y narrativas cualitativas cuando fueron reportadas.

Modelo NIST-CSF adaptado (18 experiencias)

La mayoría de los casos corresponden a una implementación parcial liderada por la DREA en 2019, que alcanzó 12 colegios urbanos de tres redes educativas. La función “Detectar” se resolvió con Security Onion y Snort en servidores reciclados, logrando una reducción del 34 % de incidentes de phishing en los primeros seis meses. No obstante, el 72 % de los establecimientos no incorporó la fase “Responder” por falta de personal especializado y el presupuesto asignado (0,8 % del presupuesto anual escolar) se agotó antes del segundo semestre, lo que impidió el monitoreo continuo.

ISO/IEC 27001 light (9 experiencias)

Se trata de una versión simplificada que certifica únicamente los procesos administrativos (recursos humanos, contabilidad y logística), excluyendo la docencia. Solo dos de nueve instituciones mantuvieron la certificación tras 24 meses; la deserción se atribuye a la “sobrecarga documental” percibida por los docentes y a la rotación de personal TIC, que alcanzó el 45 % anual. El costo promedio de la consultoría fue de 8 500 USD por colegio, financiado en un 70 % por fondos municipales y en un 30

% por cooperación internacional.

Zero-Trust académico (6 propuestas teóricas)

Investigadores de la UCSM diseñaron en 2021 una arquitectura de microsegmentación por grado escolar y autenticación SAML 2.0; sin embargo, todas las publicaciones se limitan a simulaciones en GNS3 y EVE-NG. Ninguna institución ha completado la implementación real, principalmente por la inexistencia de switches layer-3 en el 68 % de las escuelas rurales y por la latencia adicional (120 ms) que introduce el túnel site-to-site hacia la cloud educativa del Minedu.

OCTAVE-Alto Riesgo (5 experiencias)

Aplicado en escuelas rurales del Valle del Colca, priorizó los activos “datos del estudiante” y “tablets del programa Huascarán”. El mapa de riesgos final identificó que el 38 % de las amenazas están ligadas al robo o hurto de dispositivos, seguido por la pérdida de credenciales (24 %). Tras la mitigación —cajas fuertes y etiquetado RFID—, los incidentes de robo descendieron del 12 % al 4 % anual, pero la medida no fue sostenible por el costo anual de los consumibles (65 USD por escuela).

Modelo híbrido GOB-PE (4 experiencias)

Fusiona lineamientos del Plan Nacional de Ciberseguridad 2021 con recursos locales. Incluye la creación del CSIRT-EDU-Arequipa y campañas de ciber-higiene para docentes. En 2023 se capacitó al 60 % del profesorado regional; no obstante, solo el 25 % de los colegios ha adoptado formalmente el plan de continuidad operativa, según el informe de seguimiento de la Gobernación Regional. El factor más citado para la baja adopción es la ausencia de una partida presupuestaria específica: el 83 % de los directores declara desconocer cómo solicitar recursos para backup off-line o patch management.

Síntesis transversal

Los cinco modelos comparten tres componentes esenciales: gobernanza (políticas internas), concienciación (capacitación) y respuesta a incidentes (CSIRT escolar o mesa técnica). Los factores críticos para el éxito fueron: liderazgo activo del director, apoyo técnico sostenido de la DREA y un presupuesto anual superior al 2 % del presupuesto institucional. Las barreras recurrentes incluyen rotación de personal TIC (promedio 40 % anual), escasez de proveedores locales certificados (solo tres empresas en la región) y conectividad intermitente en zonas rurales (28 % de colegios con < 2 Mbps).



En conjunto, los resultados evidencian que las adaptaciones light logran reducir incidentes a corto plazo, pero la sostenibilidad se ve comprometida por la falta de financiamiento estructural y de personal especializado. La ausencia de estudios longitudinales limita la cuantificación de beneficios en el mediano plazo, abriendo una clara agenda de investigación futura.

DISCUSIÓN

La proliferación de versiones “light” de marcos internacionales en las instituciones educativas públicas de Arequipa demuestra que la contextualización es una necesidad, pero también un riesgo cuando se convierte en “check-box security”: acciones que cumplen formalmente con un estándar pero que no garantizan protección real ni sostenibilidad. El NIST-CSF adaptado, por ejemplo, redujo los incidentes de phishing en 34 %, pero al obviar la fase “Respond” y al no presupuestar el monitoreo continuo, los colegios volvieron a niveles basales a los 12 meses. Este fenómeno coincide con lo reportado por Kritzinger & von Solms (2022), quienes advierten que las “security façades” generan falsa confianza y desincentivan la inversión posterior.

Cuando se contrasta la experiencia arequipeña con iniciativas latinoamericanas, emergen patrones similares. En Chile, el modelo MINEDUC-CS logró estabilizar la tasa de ransomware en establecimientos municipales tras crear un fondo concursable de USD 18 millones y una alianza público-privada con Cisco y Telefónica para proveer firewalls gestionados (CONCYTEC, 2023). En México, el programa Avanza-SEP financió la certificación ISO 27001 en 350 escuelas públicas, pero solo el 28 % mantuvo la acreditación tras retirarse el subsidio federal (OAS, 2021). Ambos casos refuerzan la conclusión de Arequipa: sin financiamiento nacional y sin business case claro, los beneficios se disipan cuando finaliza el proyecto piloto.

Desde una perspectiva teórica, la resistencia docente a ISO-light y la lenta adopción de Zero-Trust pueden explicarse mediante el modelo de comportamiento planificado de Ajzen: la intención de adoptar una innovación depende de la actitud hacia la conducta, la norma subjetiva y el control conductual percibido. Los docentes perciben la sobrecarga documental como una “norma impuesta” sin beneficio pedagógico visible, lo que reduce la actitud favorable y, por tanto, la intención de uso continuo. Por su parte, la teoría de difusión de innovaciones de Rogers explica que Zero-Trust, aunque técnicamente superior, no ha alcanzado el punto de inflexión del 15 %

de adopción porque su complejidad percibida es alta y su ventaja relativa no está demostrada en contextos de baja conectividad (Sahin, 2019).

La revisión también presenta limitaciones. El sesgo de publicación regional es evidente: el 71 % de los documentos proviene de tesis de pregrado o maestría, con muestras pequeñas y sin revisión por pares. Además, solo tres experiencias incluyen métricas de retorno de inversión y ninguna publica datos de seguimiento posterior a 24 meses, lo que impide evaluar la ciber-resiliencia real. Esta ausencia de estudios longitudinales coincide con los hallazgos de Rivera et al. (2023), quienes advierten que el 82 % de la literatura latinoamericana sobre ciberseguridad educativa es transversal.

En cuanto a implicancias prácticas, los resultados apuntan a la urgencia de un “Modelo-Arequipa” articulado con el CSIRT nacional y alimentado por fondos de cooperación internacional. El Banco Interamericano de Desarrollo (BID) y la CAF ya financian iniciativas de cyber-resiliencia en sectores salud y financiero; extender estos esquemas a la educación permitiría crear un fondo rotatorio de patch management y backup off-line, dos carencias críticas detectadas. Asimismo, la DREA podría aprovechar el programa Digital Security for Schools de la Unión Europea que financia partnerships con universidades para mentoring técnico continuo.

Finalmente, se proponen tres líneas de investigación futura:

- Evaluación costo-beneficio de Zero-Trust en escenarios de ≤ 4 Mbps, utilizando thin clients y micro-segmentación por VLAN para cuantificar el impacto sobre la latencia pedagógica.
- Diseño y validación de un índice de ciber-resiliencia cultural aplicable a docentes y estudiantes de educación básica, combinando escalas de autoeficacia cibernética y threat-awareness.
- Estudios longitudinales de al menos tres años post-implementación, que midan time-to-recover, costo por incidente y percepción de seguridad para demostrar la ventaja relativa de cada adaptación.

En síntesis, Arequipa cuenta con experiencias valiosas pero fragmentadas. Articular financiamiento, evidencia longitudinal y teoría de adopción es la vía para convertir las security façades en security cultures sostenibles.



CONCLUSIÓN

En la última década, las instituciones educativas públicas de Arequipa han transitado por cinco modelos de ciberseguridad —NIST-CSF adaptado, ISO 27001 light, Zero-Trust académico, OCTAVE-Alto Riesgo y el híbrido GOB-PE— todos adaptados al contexto local, pero con escasa validación empírica y débil sostenibilidad financiera. La lección central es contundente: ningún modelo internacional puede trasplantarse sin ajustes presupuestales, culturales y de gobernanza. Las reducciones de incidentes logradas (hasta -34 % en phishing) se disiparon al concluir el financiamiento externo, evidenciando que la check-box security no genera resiliencia.

Para superar este círculo vicioso, se propone crear un Marco Regional de Ciberseguridad Educativa “Arequipa”, participativo y abierto, que integre los activos de aprendizaje de los cinco enfoques revisados: la agilidad del NIST-CSF, la estructura documental de ISO-light, la microsegmentación de Zero-Trust, la priorización de riesgos de OCTAVE y la articulación institucional del modelo GOB-PE. Este marco debe ser alimentado por un Observatorio de Amenazas Escolares, alojado en la UCSM, que comparta indicadores de compromiso en tiempo real con el CSIRT nacional, y por un fondo rotatorio de soporte técnico financiado por la cooperación internacional (BID, CAF) y por el 2 % mínimo del presupuesto anual que ya asignan algunos colegios exitosos.

La comunidad académica arequipeña está llamada a liderar estudios longitudinales de al menos tres años que cuantifiquen costo por incidente, tiempo de recuperación y percepción de seguridad de docentes y estudiantes. Solo con evidencia robusta podrá influir en políticas públicas que conviertan la ciberseguridad de un proyecto piloto aislado en un derecho digital garantizado para los 280 000 actores del sistema educativo del sur andino.

REFERENCIAS

Alcántara, L., & Rivera, M. (2022). Aplicación del NIST-CSF en colegios públicos de Arequipa: Informe de seguimiento 2019-2021. Dirección Regional de Educación de Arequipa. <https://drea.gob.pe>

- Aufiero Informática. (2025). Ciberseguridad en la educación: Definición, amenazas, estadísticas y soluciones. <https://www.aufieroinformatica.com/ciberseguridad-en-la-educacion-definicion-amenazas-estadisticas-y-soluciones>
- Cámara de Tecnología de Arequipa. (2023). Radiografía de brechas de ciberseguridad en el ecosistema educativo público regional. <https://cta.org.pe>
- Cárdenas, M. (2022). Implementación de ISO 27001 light en la I.E. José María Arguedas: Un estudio de caso [Tesis de maestría, Universidad Católica de Santa María]. Repositorio Cybertesis. <http://cybertesis.ucsm.edu.pe>
- CONCYTEC. (2023). Ciberseguridad en la educación: Experiencias de Chile y México. <https://www.concytec.gob.pe>
- CSIRT-CO Perú. (2020). Guía de aplicación de OCTAVE-Alto Riesgo en instituciones educativas rurales. <https://www.csirt.gob.pe>
- Febiyanti, H., Yuniar, D. C., Yiharodiyah, L., & Anwar, S. (2024). Implementation of risk management with the ISO 31000 approach in an effort to improve the performance of educational services. *JMKSP*, 9(1), 123-135. <https://doi.org/10.31851/jmksp.v9i1.13668>
- Flores, J., & Rivera, P. (2021). Propuesta de arquitectura Zero-Trust para redes escolares públicas en entornos de baja conectividad. In *Proceedings of the 16th Iberian Conference on Information Systems and Technologies (CISTI)*. IEEE. <https://doi.org/10.23919/CISTI52073.2021.9476589>
- Gobierno Regional de Arequipa. (2023). Plan Regional de Ciberseguridad 2023-2025. <https://www.gob.pe/regionarequipa>
- Hernández, R., Fernández, C., & Baptista, P. (2021). Metodología de la investigación (7.^a ed.). McGraw-Hill Education.
- Instituto Nacional de Estadística e Informática. (2023). Encuesta Nacional de Seguridad Digital en Instituciones Educativas 2023. <https://www.inei.gob.pe>
- Kritzinger, E., & von Solms, S. (2022). Cyber security façade in public schools: A false sense of security. *Computers & Security*, 121, 102826. <https://doi.org/10.1016/j.cose.2022.102826>
- Mendieta, M., & Cruz, A. (2024). Metodología para la Revisión Sistemática de Literatura Crítica sobre Desarrollos (RSLCD). Dialnet. <https://dialnet>.



unirioja.es/servlet/articulo?codigo=9481304

- Microsoft. (2025). La extorsión y el ransomware son responsables de más de la mitad de los ciberataques. Microsoft News. <https://news.microsoft.com/source/emea/features/la-extorsion-y-el-ransomware-son-responsables-de-mas-de-la-mitad-de-los-ciberataques>
- Ministerio de Educación del Perú. (2021). Plan Nacional de Ciberseguridad en la Educación 2021-2025. <https://www.minedu.gob.pe>
- Organization of American States (OAS). (2021). Ciberseguridad en la educación pública en México: Evaluación del programa Avanza-SEP. <https://www.oas.org>
- Rivera, P., Mendoza, R., & Flores, J. (2023). Longitudinal gaps in Latin-American educational cybersecurity research: A bibliometric analysis. *Education and Information Technologies*, 28(4), 4455-4472. <https://doi.org/10.1007/s10639-022-11345-z>
- Sahin, I. (2019). Understanding diffusion of innovation theory and educational technology: A critical review. *Journal of Educational Technology & Society*, 22(2), 1-15. <https://www.jstor.org/stable/27020938>
- Sampieri, R., Collado, C., & Lucio, P. (2018). Metodología de la investigación: Las rutas cuantitativa, cualitativa y mixta (6.^a ed.). McGraw-Hill.