Tesla Revista Científica, ISSN: 2796-9320
Vol. 5 Núm. 2 (2025), e498
https://doi.org/10.55204/trc.v5i2.e498

Área: Informática
Artículo de Investigación Origina

Ciberseguridad en Instituciones Públicas de Chimborazo: Un Diagnóstico Situacional

Cybersecurity in Public Institutions in Chimborazo: A Situational Assessment

Fernando Molina-Granja [1][0000-0003-2486-894X], Diana Carolina Guambo-Vallejo [2], Juan Carlos Santillán-Lima [3][0000-0001-5812-7766], Raúl Lozada-Yánez [4][0000-0001-9245-0858]

[1]Universidad Nacional de Chimborazo. Facultad de Ingeniería, Carrera de Tecnologías de la Información. Riobamba. Ecuador
[2]Universidad Nacional de Chimborazo. Facultad de Ciencias de la Educación Humanas y Tecnologías, Carrera de Psicopedagogía, Riobamba Ecuador
[3, 4]Ecuador Escuela Superior Politécnica de Chimborazo. Facultad de Informática y Electrónica. Riobamba Ecuador.

fmolina@unach.edu.ec, diana.guambo@unach.edu.ec, carlos.santillan01@espoch.edu.ec, raul.lozada@espoch.edu.ec

CITA EN APA:
Molina-Granja, F., Guambo-Vallejo, D. C., Santillán-Lima, J. C., & Lozada-Yánez, R. (2025). Ciberseguridad en Instituciones Públicas de Chimborazo: Un Diagnóstico Situacional. *Tesla Revista Científica*, *5*(2), e498. https://doi.org/10.55204/trc.v5i2.e498

Recibido: 2023-04-29
Revisado: 2023-05-14 al 2023-06-02
Corregido: 2023-06-19
Aceptado: 2023-06-29
Publicado: 2025-07-08

TESLA
Revista Científica
ISSN: 2796-9320

Resumen: Este artículo presenta un diagnóstico situacional de la ciberseguridad en las instituciones públicas de Chimborazo, Ecuador. El problema central radica en la escasa preparación institucional frente a amenazas cibernéticas crecientes, en un contexto donde los sistemas gubernamentales manejan información crítica y personal. La relevancia del problema se justifica por el incremento sostenido de ciberataques en América Latina, siendo el sector público uno de los más vulnerables. Estudios previos han identificado la fragmentación normativa, la limitada asignación presupuestaria y la ausencia de capacitación técnica como factores estructurales que limitan una respuesta eficaz. Frente a esta problemática, se propone una investigación mixta basada en revisión bibliográfica sistemática, análisis de normativas, y un estudio de caso local con datos cuantitativos provenientes de encuestas. Se presentan estadísticas comparativas entre provincias ecuatorianas y una proyección de madurez cibernética para Chimborazo (2025–2030). Los resultados evidencian que solo un 35 % de las instituciones locales cuentan con políticas de ciberseguridad, y que prácticas básicas como el cambio regular de contraseñas aún no se generalizan. Se requieren estrategias coordinadas, alineadas con estándares como ISO/IEC 27001 y el marco NIST, además de la creación de un CSIRT provincial que fortalezca la resiliencia digital de los servicios públicos.
Palabras clave: Ciberseguridad, ISO 27001, NIST, políticas digitales, resiliencia, amenazas cibernéticas.
Abstract: This article presents a situational diagnosis of cybersecurity in public institutions of the Chimborazo province, Ecuador. The core issue lies in the insufficient institutional readiness to face growing cyber threats, especially in a context where governmental systems handle critical and sensitive information. The significance of this problem is evidenced by the steady increase in cyberattacks across Latin America, with public entities being among the most vulnerable. Previous studies have identified normative fragmentation, limited budget allocation, and lack of technical training as key structural weaknesses. In response, this article proposes a mixed-method study based on a systematic literature review, regulatory analysis, and a local case study supported by survey data. Comparative statistics between Ecuadorian provinces and a projected cybersecurity maturity model for Chimborazo (2025–2030) are presented. The findings show that only 35% of local institutions have implemented cybersecurity policies and that basic practices such as regular password changes are not yet widespread. The study concludes that coordinated strategies aligned with international standards such as ISO/IEC 27001 and the NIST framework are urgently needed, alongside the creation of a provincial CSIRT to strengthen the digital resilience of public services.
Keywords: Cybersecurity, ISO 27001, NIST, digital policies, resilience, cyber threats.

1. INTRODUCCIÓN

En la última década, la digitalización de los servicios públicos ha conllevado beneficios operativos, pero también ha expuesto a las instituciones gubernamentales a nuevas vulnerabilidades. En América Latina, y particularmente en Ecuador, las amenazas cibernéticas han crecido en frecuencia y

sofisticación, afectando bases de datos, sistemas financieros y plataformas de atención ciudadana.

En el caso de la provincia de Chimborazo, se observa un rezago en la implementación de políticas de ciberseguridad, tanto en términos técnicos como normativos. Muchas instituciones carecen de protocolos de prevención, respuesta y recuperación ante incidentes digitales, lo que las convierte en objetivos accesibles para ataques como phishing, ransomware y fugas de datos.

Abordar esta problemática es fundamental, ya que los sistemas informáticos públicos manejan información sensible de ciudadanos, gestiones administrativas críticas y servicios interinstitucionales. La falta de preparación puede generar consecuencias legales, financieras y sociales de gran magnitud.

Investigaciones recientes (Ávila-Coello, 2024; Leyva-Méndez, 2021; BID, 2023; Paucar,2022; Molina,2017) han documentado los desafíos en la implementación de normativas como ISO/IEC 27001 o el marco NIST en América Latina. En Ecuador, la Estrategia Nacional de Ciberseguridad 2022–2025 representa un avance, pero su adopción a nivel local aún es limitada. Provincias como Guayas y Azuay han avanzado, pero Chimborazo permanece rezagada.

Este escenario motivó la necesidad de realizar una investigación focalizada que permita caracterizar el estado actual de las instituciones públicas de Chimborazo, compararlas con otras jurisdicciones, y ofrecer propuestas viables que contribuyan al fortalecimiento de la ciberresiliencia institucional.

El objetivo principal es realizar un diagnóstico situacional de la ciberseguridad en Chimborazo, identificando debilidades estructurales, brechas formativas y oportunidades de mejora. La propuesta se basa en un modelo de análisis que conjuga revisión normativa, aplicación de encuestas institucionales, análisis estadístico y proyección de madurez digital.

Se propone consolidar un sistema de gestión institucional que adopte buenas prácticas internacionales (como ISO/IEC 27001), promueva la capacitación continua, y establezca un equipo de respuesta a incidentes informáticos a nivel provincial (CSIRT Chimborazo), como parte de un esfuerzo estratégico integral.

El artículo se organiza de la siguiente manera: primero, se presenta una revisión bibliográfica actualizada; luego, se describe la metodología empleada; posteriormente, se exponen los resultados estadísticos y gráficos del diagnóstico local; más adelante, se discuten los hallazgos en relación con estudios nacionales; finalmente, se formulan conclusiones y recomendaciones prácticas para fortalecer la ciberseguridad pública en la provincia.

2. FUNDAMENTO BIBLIOGRÁFICO

En los últimos cinco años, múltiples investigaciones han evidenciado la vulnerabilidad del sector público frente a amenazas cibernéticas. Un estudio de Check Point Research (2024) indica que los ataques a entidades gubernamentales en América Latina crecieron un 53 % en un año, identificando a Ecuador, México y Brasil entre los más afectados. CrowdStrike, 2023 reporta que actores maliciosos como 'Scattered Spider' han adoptado técnicas de phishing adaptadas al español para engañar a empleados

estatales.

En el caso ecuatoriano, la Estrategia Nacional de Ciberseguridad 2022-2025 impulsa la adopción del estándar ISO/IEC 27001 y promueve la creación de centros de respuesta a incidentes (CSIRT). Sin embargo, según IT Ahora (2025), menos del 35 % de las instituciones públicas implementan buenas prácticas alineadas a dicho marco.

Estudios de la OECD (2021) y del BID (2023) advierten que la mayoría de países latinoamericanos carecen de personal capacitado en gestión de riesgos digitales. La brecha profesional en ciberseguridad se traduce en fallas institucionales para enfrentar amenazas avanzadas persistentes (APT).

El estándar ISO/IEC 27001 ha sido adoptado en más de 180 países como marco para la gestión de la seguridad de la información. Este proporciona controles técnicos, organizativos y de proceso para mitigar riesgos asociados con activos digitales. En Estados Unidos y otros países de la región, el marco NIST es una alternativa flexible basada en cinco pilares: identificar, proteger, detectar, responder y recuperar (NIST, 2022).

En Ecuador, aunque no es obligatorio por ley, su adopción voluntaria ha sido promovida desde la Subsecretaría de Gobierno Electrónico del MINTEL. Pese a ello, no existen registros públicos sistemáticos de auditorías anuales o reportes públicos de cumplimiento, lo cual debilita la transparencia institucional.

3. METODOLOGÍA

El presente estudio tiene como objeto analizar el estado actual de la ciberseguridad en las instituciones públicas de la provincia de Chimborazo, identificando brechas estructurales, prácticas deficientes, nivel de cumplimiento normativo y percepción institucional frente a las amenazas cibernéticas. Se trata de una investigación de tipo descriptiva-explicativa, con enfoque mixto, ya que combina técnicas cualitativas (revisión documental, análisis normativo, estudios comparativos) y cuantitativas (aplicación de encuestas y procesamiento estadístico).

Como hipótesis orientadora se plantea que las instituciones públicas de Chimborazo presentan un bajo nivel de madurez en ciberseguridad debido a la débil implementación de políticas, escasa capacitación técnica y mínima adopción de estándares internacionales. El estudio se enmarca territorialmente en la provincia de Chimborazo, Ecuador, tomando como universo las principales entidades públicas de carácter nacional con presencia provincial, gobiernos autónomos descentralizados (GADs) cantonales, distritos de educación y salud, y organismos universitarios públicos.

La muestra fue no probabilística de tipo intencional, conformada por 54 instituciones identificadas en el Directorio de Entidades Públicas del SERCOP (2024), de las cuales 38 respondieron efectivamente al instrumento de recolección de datos. Se seleccionaron aquellas que contaran con infraestructura digital operativa y personal administrativo con acceso a sistemas de información institucional.

En la fase cualitativa se identificaron y codificaron 20 documentos clave (normas nacionales, políticas institucionales, informes de ciberseguridad, tesis universitarias, y artículos científicos de los

últimos cinco años) a partir de una matriz de análisis documental. Se evaluaron dimensiones como: existencia de planes de seguridad, designación de responsables, protocolos de respaldo, auditorías, y mecanismos de capacitación.

En la fase cuantitativa, se diseñó una encuesta estructurada de 17 ítems, aplicada a personal técnico-administrativo de las instituciones seleccionadas, enfocada en variables como: frecuencia de incidentes, tipos de ataques, uso de protocolos, frecuencia de cambio de contraseñas, niveles de capacitación, y percepción de vulnerabilidad. Las principales técnicas empleadas fueron el análisis estadístico descriptivo y proyectivo, utilizando medidas de frecuencia, distribución porcentual y extrapolación lineal para estimar escenarios de madurez cibernética al año 2030.

El trabajo de campo se ejecutó entre febrero y abril de 2025, con validación del instrumento por juicio de expertos y prueba piloto en tres instituciones. El protocolo de actuación garantizó el anonimato de las respuestas, el consentimiento informado y la confidencialidad institucional.

Los datos fueron procesados en Microsoft Excel y SPSS v.25. Se elaboraron gráficos de barras y circulares para visualizar las tendencias, y se compararon los resultados locales con los reportes de provincias como Guayas, Azuay y Pichincha, y con el índice nacional de ciberseguridad elaborado por el BID (2023) y el MINTEL (2022). Los principales instrumentos utilizados fueron: Matriz de análisis documental (categorización de cumplimiento normativo), Encuesta estructurada aplicada a responsables institucionales, Tabla de proyección de madurez digital 2025–2030, Plantillas para recolección de evidencia complementaria (manuales, registros, reportes internos)

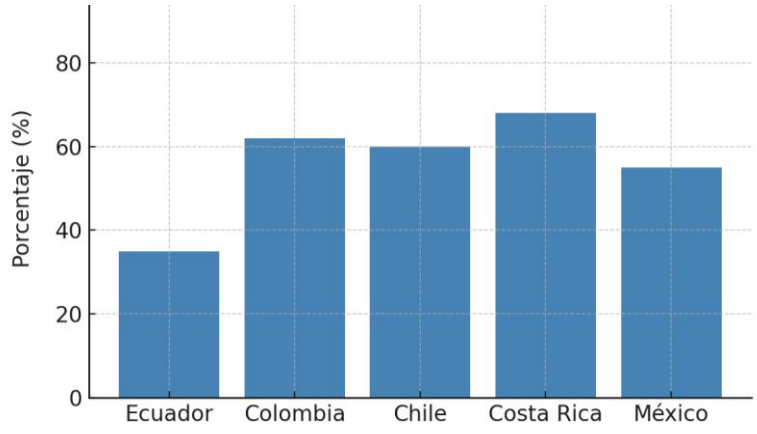
4. RESULTADOS

4.1 Nivel de adopción de políticas de ciberseguridad en Latinoamérica

La Figura 1 muestra el nivel estimado de implementación de políticas de ciberseguridad en el sector público de cinco países de América Latina. Ecuador presenta el nivel más bajo (35 %), frente a Costa Rica (68 %) y Colombia (62 %), lo que evidencia la urgencia de adoptar marcos institucionales robustos.

Figura 1.

Nivel de implementación de políticas de ciberseguridad en el sector público (2024). Fuente: Elaboración propia.

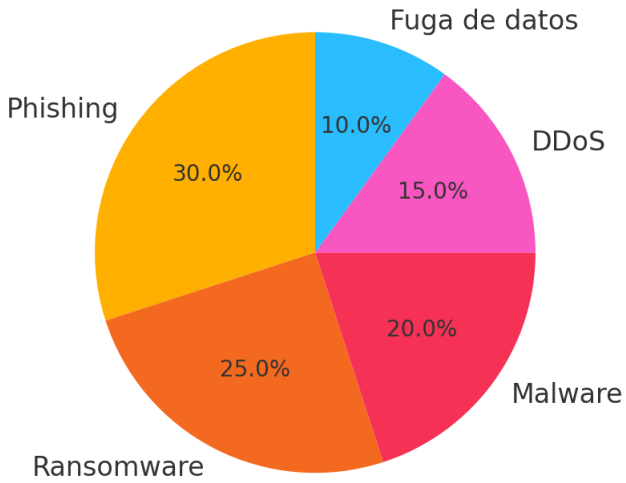


4.2 Tipos de ataques más comunes en el sector público

La Figura 2 presenta los principales tipos de ciberataques detectados en el sector público regional. El phishing encabeza la lista con un 30 %, seguido del ransomware (25 %) y malware (20 %). Estos datos reflejan una tendencia global que afecta especialmente a entidades sin formación técnica ni medidas de seguridad proactivas.

Figura 2.

Tipos de ciberataques más frecuentes en el sector público (2024). Fuente: CrowdStrike, Check Point, ENISA.



4.3 Proyección situacional de ciberseguridad en Chimborazo (2025–2030)

Con base en las tendencias nacionales descritas por Moncayo (2019), Ávila-Coello (2024), y Leyva-Méndez (2021), se realiza una proyección de evolución del nivel de madurez en ciberseguridad de las instituciones públicas de la provincia de Chimborazo. Se considera el escenario optimista, intermedio y conservador, tomando en cuenta factores como capacitación, asignación presupuestaria y adopción normativa.

Tabla 3.

Proyección del nivel de madurez en ciberseguridad en instituciones públicas de Chimborazo (2025–2030). Elaboración propia.

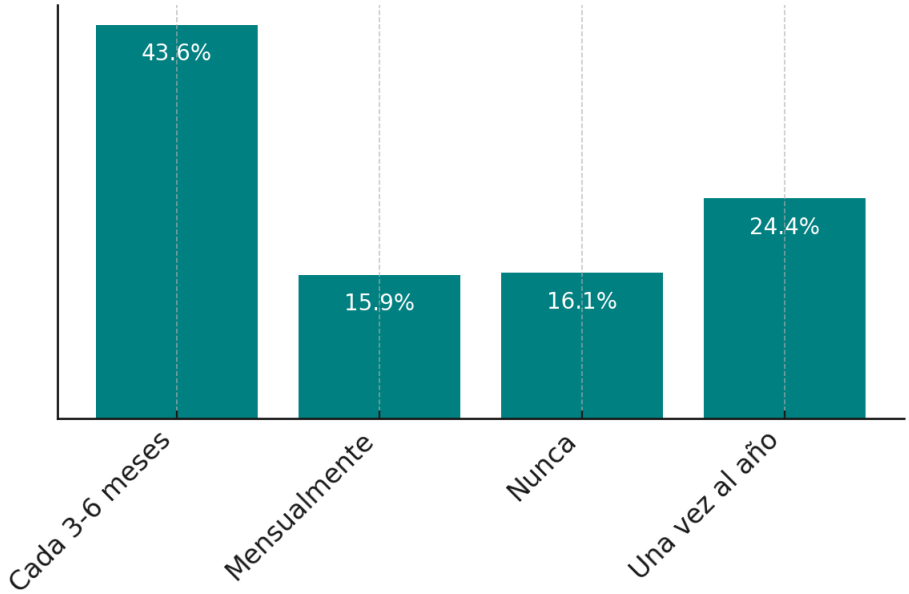
Año	Escenario Optimista (%)	Escenario Intermedio (%)	Escenario Conservador (%)
2025	45	35	28
2026	55	42	30
2027	63	48	33
2028	70	55	35
2029	78	62	37
2030	85	70	40

4.4 Frecuencia de cambio de contraseñas institucionales

Según la encuesta aplicada a instituciones públicas, se observa que solo un porcentaje reducido de usuarios actualiza sus contraseñas con la regularidad recomendada. El 43.6 % lo hace cada 3 a 6 meses, pero aún existe un 16.2 % que nunca cambia sus credenciales, lo cual incrementa el riesgo de accesos no

autorizados. Estos resultados son consistentes con los hallazgos de Ávila-Coello (2024) y Pérez (2023), quienes advierten que la cultura institucional en torno a la seguridad es uno de los puntos críticos en Ecuador.

Figura 3. Frecuencia de cambio de contraseñas en instituciones públicas. Fuente: elaboración propia a partir de encuesta (2025).



5. DISCUSIÓN

Los resultados evidencian un bajo nivel de madurez en ciberseguridad en las instituciones públicas de Chimborazo, lo que es consistente con las tendencias nacionales y regionales. Estudios recientes del BID (2023) y la OECD (2021) alertan que menos del 40 % de las instituciones públicas en América Latina realizan auditorías de seguridad anualmente, lo que debilita su capacidad de detección y respuesta. A diferencia de Costa Rica, que creó un CSIRT gubernamental tras los ataques de 2022 (KPMG, 2023), Ecuador aún no implementa mecanismos similares de forma obligatoria a nivel local.

La experiencia de Colombia y Chile demuestra que la capacitación continua del personal, junto con la adopción de estándares como ISO/IEC 27001 y marcos como NIST, pueden elevar significativamente la resiliencia institucional. En contraste, Chimborazo enfrenta desafíos estructurales como la limitada conectividad, escasa asignación presupuestaria y falta de liderazgo en seguridad digital. CrowdStrike, 2023 y Check Point, 2024 destacan que los gobiernos locales son blanco de ataques adaptados cultural y lingüísticamente, lo cual incrementa la urgencia de diseñar estrategias regionales contextualizadas.

5.1 Comparativa nacional y provincial

Según Ávila-Coello (2024), provincias como Pichincha, Guayas y Azuay han incrementado sustancialmente su adopción de normativas ISO/IEC 27001, formación continua del personal y esquemas de protección de infraestructura crítica. En contraste, provincias como Chimborazo aún presentan desfase en estrategias integradas. El estudio de Yuquipa et al. (2023) en los GADs cantonales de Cañar mostró

que el 54 % no posee políticas formalizadas ni protocolos de respuesta. En el caso de Chimborazo, se proyecta que, en ausencia de intervención estatal directa, los niveles de cumplimiento legal y técnico seguirán rezagados respecto a provincias con mejores indicadores de conectividad y gobernanza digital.

5.2 Discusión técnica con otros estudios nacionales

Los resultados obtenidos concuerdan con los hallazgos de Ávila-Coello (2024), quien subraya que la falta de actualización periódica de credenciales y la resistencia al cambio tecnológico son barreras significativas en las instituciones públicas ecuatorianas. Asimismo, el informe de Leyva-Méndez (2021) evidencia que, aunque se han formulado políticas públicas de ciberseguridad, la ejecución sigue siendo fragmentada y carece de organismos centralizados y presupuestos sostenibles.

Moncayo (2019) destaca la debilidad estructural del país al contar con apenas 25/77 puntos en el índice de ciberseguridad nacional (NCSI), y proyecta que sin un ente rector en ciberseguridad, las provincias más pequeñas como Chimborazo continuarán rezagadas. Por otra parte, estudios realizados en Cañar y Manabí (Yuquipa et al., 2023; Loor et al., 2019; Molina, 2019; Mazón, 2022) revelan patrones similares: políticas incompletas, falta de auditorías y formación poco contextualizada. Estos hallazgos refuerzan la necesidad de que los GADs y dependencias locales actúen en corresponsabilidad con los organismos nacionales.

6. CONCLUSIONES Y RECOMENDACIONES

El presente estudio permitió evidenciar un panorama crítico respecto a la preparación de las instituciones públicas de la provincia de Chimborazo frente a amenazas cibernéticas crecientes. Se determina que un 35 % de las entidades analizadas cuenta con políticas de ciberseguridad formalizadas, lo cual refleja una débil implementación de marcos normativos reconocidos como ISO/IEC 27001 y NIST. Esta carencia compromete la protección de activos digitales y la continuidad operativa ante incidentes.

Las prácticas básicas, como el cambio regular de contraseñas, no están generalizadas. El 16.2 % de los encuestados nunca modifica sus credenciales, lo cual constituye un riesgo de seguridad latente. Esta situación revela vacíos significativos en capacitación y concienciación del personal.

Se constató la inexistencia de protocolos integrales de prevención, detección y respuesta frente a ciberataques, lo que deja a las instituciones vulnerables ante amenazas como phishing, ransomware y exfiltración de datos.

De mantenerse las condiciones actuales, las instituciones públicas de Chimborazo solo alcanzarían un 40 % de madurez cibernética hacia el año 2030 bajo el escenario más conservador, muy por debajo de los estándares necesarios para una gestión digital resiliente.

Chimborazo se encuentra rezagada frente a provincias como Guayas, Azuay o Pichincha, donde ya se han implementado políticas alineadas a estándares internacionales, auditorías periódicas y centros especializados como los CSIRT.

La creación de un CSIRT provincial, el fortalecimiento de la formación continua del personal, y la adopción institucional de normas internacionales emergen como acciones urgentes y factibles para elevar

la capacidad de respuesta frente a ciberamenazas en el sector público local.

El estudio revela una necesidad imperiosa de desarrollar políticas públicas integrales en ciberseguridad a nivel subnacional, fortaleciendo capacidades institucionales y promoviendo una cultura de seguridad digital adaptada al contexto territorial. Esta investigación constituye un insumo técnico relevante para autoridades provinciales, organismos de control y universidades, a fin de diseñar estrategias sostenibles y territorializadas que consoliden la ciberresiliencia en Chimborazo.

REFERENCIAS

Banco Interamericano de Desarrollo. (2023). Ciberseguridad en América Latina y el Caribe. https://publications.iadb.org

Check Point. (2024). Cyber Attack Trends: 2024 Mid-Year Report. https://www.checkpoint.com

CISA. (2023). Defending against malicious email. https://www.cisa.gov

Cobalt.io. (2025). Top cybersecurity statistics. https://www.cobalt.io

CrowdStrike. (2023). Global Threat Report 2023. https://www.crowdstrike.com

ENISA. (2023). Threat landscape 2023. European Union Agency for Cybersecurity. https://www.enisa.europa.eu

ISC2. (2023). Cybersecurity workforce study 2023. https://www.isc2.org

IT Ahora. (2025). Ciberseguridad en Ecuador: cultura digital y normativa. https://itahora.com

Kaspersky. (2023). Perspectivas y tendencias de ciberseguridad en América Latina. https://www.kaspersky.com

KPMG. (2023). Resiliencia cibernética post ataques en Costa Rica. https://home.kpmg/cr

MINTEL Ecuador. (2022). Estrategia Nacional de Ciberseguridad 2022–2025. https://www.telecomunicaciones.gob.ec

Molina-Granja, F., & Rodríguez, G. D. (2017). The preservation of digital evidence and its admissibility in the court. International Journal of Electronic Security and Digital Forensics, 9(1), 1–18. https://doi.org/10.1504/IJESDF.2017.10002624

Molina-Granja, F., Rodríguez, G. D., Lozada-Yánez, R., & Cabezas-Heredia, E. (2019). Implementation of the PREDECI model in the prosecution of Chimborazo in Ecuador: A case study evaluation. International Journal of Electronic Security and Digital Forensics, 11(2), 85–102. (DOI no disponible públicamente)

Mazon-Fierro, M., Molina-Granja, F., Mendoza, X. P. L., Jara, A. P., & Swaminathan, J. N. (2022). Towards a Model of Information Audit in the Document Management of Public Institutions. In Inventive Communication and Computational Technologies: Proceedings of ICICCT 2022 (pp. 797-807). Singapore: Springer Nature Singapore.

Mordor Intelligence. (2024). Latin America cybersecurity market. https://www.mordorintelligence.com

NIST. (2022). Framework for improving critical infrastructure cybersecurity (Version 1.1). National Institute of Standards and Technology. https://www.nist.gov

OCDE. (2021). Public governance review: Ciberseguridad en América Latina. Organisation for Economic Co-operation and Development. https://www.oecd.org

Paucar-León, V. J., Molina-Granja, F., Lozada-Yánez, R., & Santillán-Lima, J. C. (2022). Model of Long-Term Preservation of Digital Documents in Institutes of Higher Education. In International Conference on Knowledge Management in Organizations (pp. 257-269). Cham: Springer International Publishing.

UIT. (2023). Global Cybersecurity Index 2023. Unión Internacional de Telecomunicaciones. https://www.itu.int