BET-EL INVESTIGIUM
Revista Multidiciplinar

ISSN: 3121-259X

MÉTODOS Y EVIDENCIA

VOL.2, Nº2 (julio –diciembre, 2025)

ISSN: 3121-259X

DOI: https://doi.org/10.70577/bvvjb559

Fecha de recepción: 11/08/2025

Fecha de aceptación: 19/11/2025

Fecha de publicación: 12/12/2025

Ciencia y seguridad: protección de infraestructuras, riesgos laborales y ciberdefensa en la provincia de Santo Domingo Tsáchila

"Science and Security: Infrastructure Protection, Occupational Risks, and Cyber Defense in the Tsáchila Province"

Ángel Hernán Marín Cepeda
Instituto Superior Tecnológico Bet-El
hernanmarin@bet-el.edu.ec
https://orcid.org/0000-0002-3216-8217
Ecuador – Santo Domingo de los Tsáchilas

Citación

Marín, A. (2025). Ciencia y seguridad: protección de infraestructuras, riesgos laborales y ciberdefensa en la provincia de Santo Domingo Tsáchila Revista Investigium. 2(2), p. 32 – 44.

ISSN: 3121-259X

RESUMEN

La seguridad integral constituye un desafío prioritario en contextos territoriales caracterizados por dinámicas productivas complejas y crecientes riesgos físicos, laborales y digitales. En este marco, el estudio analiza la seguridad integral desde una perspectiva multidimensional, integrando la protección de infraestructuras, la seguridad laboral y la ciberseguridad en la provincia de Santo Domingo de los Tsáchilas, Ecuador, con el propósito de identificar brechas y desafíos en su gestión. La investigación se desarrolló bajo un enfoque mixto, con diseño descriptivo y no experimental, utilizando revisión documental, análisis normativo y evaluación contextual de prácticas organizacionales. Los resultados evidencian que la protección de infraestructuras se gestiona principalmente de manera reactiva, con limitada planificación preventiva; la seguridad laboral presenta debilidades en la cultura preventiva y en la aplicación sistemática de controles; y la ciberseguridad muestra bajos niveles de madurez en la gestión de incidentes. La discusión permite interpretar estos hallazgos como resultado de una gestión fragmentada de los riesgos, en coherencia con estudios previos que señalan dificultades en la implementación operativa de la seguridad integral a nivel local. Se concluye que la seguridad integral requiere modelos sistémicos e integrados que articulen dimensiones físicas, humanas y digitales, aportando evidencia científica contextualizada para fortalecer la resiliencia organizacional y territorial.

Palabras clave: seguridad integral; protección de infraestructuras; seguridad laboral; ciberseguridad.

ISSN: 3121-259X

ABSTRACT

Integral security represents a priority challenge in territorial contexts characterized by complex productive dynamics and increasing physical, occupational, and digital risks. Within this framework, this study analyzes integral security from a multidimensional perspective, integrating infrastructure protection, occupational safety, and cybersecurity in the province of Santo Domingo de los Tsáchilas, Ecuador, with the aim of identifying gaps and challenges in its management. The research was conducted using a mixed-methods approach with a descriptive, non-experimental design, based on documentary review, regulatory analysis, and contextual evaluation of organizational practices. The results indicate that infrastructure protection is mainly managed through reactive approaches with limited preventive planning; occupational safety shows weaknesses in preventive culture and systematic control application; and cybersecurity exhibits low levels of maturity in incident management. The discussion interprets these findings as a consequence of fragmented risk management, consistent with previous studies that highlight difficulties in the operational implementation of integral security at the local level. The study concludes that integral security requires systemic and integrated models that articulate physical, human, and digital dimensions, providing contextualized scientific evidence to strengthen organizational and territorial resilience.

Keywords: integral security; infrastructure protection; occupational safety; cybersecurity.

ISSN: 3121-259X

INTRODUCCIÓN

La seguridad se consolida en la actualidad como un concepto estratégico de alcance multidimensional, estrechamente vinculado a la protección de las personas, las organizaciones y los entornos físicos y digitales en los que se desarrollan las actividades sociales y productivas. En este contexto, la noción de seguridad integral adquiere especial relevancia, al superar enfoques tradicionales centrados exclusivamente en la defensa del Estado y orientarse hacia la protección del individuo, la infraestructura, el trabajo y la información en un entorno caracterizado por riesgos complejos y dinámicos (Lucio Vásquez, 2020).

En el ámbito latinoamericano y ecuatoriano, la seguridad integral se encuentra formalmente reconocida como un eje de la política pública, especialmente a partir de la Constitución de la República del Ecuador de 2008. Este enfoque incorpora dimensiones físicas, humanas, sociales y tecnológicas, y responde a amenazas emergentes derivadas de la globalización, la transformación productiva y la digitalización de los procesos organizacionales (Lucio Vásquez, 2020). Sin embargo, diversos estudios advierten que la consolidación de este paradigma enfrenta dificultades en su aplicación práctica, particularmente a nivel local y organizacional.

Desde una perspectiva macro, la protección de infraestructuras críticas se vincula directamente con la continuidad operativa, la resiliencia territorial y el desarrollo económico. A nivel meso, la seguridad y salud en el trabajo constituye un componente esencial de la seguridad integral, al incidir en la productividad, el bienestar y la sostenibilidad de los sistemas laborales. En el caso ecuatoriano, se ha evidenciado la persistencia de riesgos ocupacionales, subregistro de accidentes y limitaciones en los mecanismos de control e inspección, lo que debilita la efectividad de los sistemas preventivos (Gómez García, 2021). Estas problemáticas adquieren particular relevancia en provincias con alta actividad productiva y crecimiento urbano acelerado, como Santo Domingo de los Tsáchilas.

En el nivel micro, la ciberseguridad emerge como un eje transversal de la seguridad integral, debido a la creciente dependencia de las tecnologías de la información y la exposición a incidentes digitales que afectan tanto a infraestructuras físicas como a procesos laborales. Investigaciones recientes señalan que, si bien las organizaciones perciben un cierto grado de preparación frente a los ciberataques, en la práctica presentan bajos niveles de madurez en la gestión de incidentes, ausencia de metodologías estructuradas y limitada integración con los sistemas de gestión de riesgos (Panche Abril et al., 2022). Esta situación incrementa la vulnerabilidad organizacional y compromete la protección de activos críticos.

ISSN: 3121-259X

En este marco, palabras clave como seguridad integral, protección de infraestructuras, seguridad laboral, riesgos ocupacionales, ciberseguridad y gestión de incidentes articulan el análisis desde una visión macro–meso–micro, permitiendo comprender la interdependencia entre los distintos niveles de riesgo. No obstante, la literatura evidencia una limitada producción científica que aborde estas dimensiones de forma integrada y contextualizada a realidades territoriales específicas en el Ecuador.

Por ello, el propósito principal de este trabajo es analizar la seguridad integral desde una perspectiva multidimensional, integrando la protección de infraestructuras, la seguridad laboral y la ciberseguridad en el contexto de la provincia de Santo Domingo de los Tsáchilas, con el fin de identificar brechas, desafíos y oportunidades de mejora. El estudio busca aportar evidencia científica que contribuya a la comprensión y fortalecimiento de modelos integrados de seguridad, relevantes tanto para el ámbito académico como para la toma de decisiones institucionales y territoriales.

MÉTODOS Y MATERIALES

El estudio se desarrolló bajo un enfoque metodológico mixto, de tipo descriptivo–analítico, con un diseño no experimental y transversal, orientado a analizar la seguridad integral desde tres dimensiones: protección de infraestructuras, seguridad laboral y ciberseguridad, en el contexto de la provincia de Santo Domingo de los Tsáchilas, Ecuador. La investigación se estructuró mediante un enfoque cualitativo y cuantitativo. El componente cualitativo permitió interpretar el marco normativo, institucional y organizacional relacionado con la seguridad integral, mientras que el componente cuantitativo facilitó la identificación de tendencias, niveles de riesgo y brechas existentes en los entornos laborales y de infraestructura analizados. El diseño fue transversal, dado que la información se recopiló en un período específico, sin manipulación deliberada de variables.

La población de estudio estuvo constituida por instituciones públicas, empresas privadas y organizaciones productivas localizadas en la provincia de Santo Domingo de los Tsáchilas, cuyos procesos operativos involucraron infraestructura física, condiciones laborales y sistemas de información digital. La unidad de análisis correspondió a los sistemas de gestión de seguridad, las condiciones de trabajo y las medidas de protección tecnológica implementadas en dichas organizaciones. Revisión documental, aplicada a normativas nacionales, resoluciones vigentes y literatura científica relacionada con seguridad y salud en el trabajo, gestión de riesgos e infraestructura crítica, tomando como referencia los lineamientos establecidos en Ecuador y estudios previos sobre siniestralidad laboral y sistemas de gestión preventiva.

Análisis de informes técnicos y estadísticos, provenientes de organismos oficiales y registros institucionales, con el fin de identificar patrones de riesgos laborales, debilidades en

ISSN: 3121-259X

la protección de infraestructuras y desafíos asociados a la seguridad digital. Listas de verificación estructuradas, diseñadas para evaluar el cumplimiento de medidas básicas de seguridad física, ocupacional y cibernética, basadas en criterios ampliamente utilizados en sistemas de gestión de seguridad y salud en el trabajo. Los instrumentos fueron elaborados específicamente para este estudio, siguiendo criterios de claridad, coherencia y validez de contenido, permitiendo su futura reutilización en contextos similares.

El procedimiento metodológico se desarrolló en las siguientes fases:

Identificación del marco teórico y normativo, mediante la revisión exhaustiva de literatura científica y normativa nacional relacionada con seguridad laboral, gestión de riesgos y prevención, considerando la evolución de los sistemas de seguridad y salud en el trabajo en Ecuador. Caracterización del contexto provincial, analizando las particularidades socioeconómicas, productivas y organizacionales de la provincia de Santo Domingo de los Tsáchilas. Aplicación de los instrumentos de evaluación, recopilando información sobre infraestructura, condiciones laborales y prácticas de ciberseguridad. Análisis e integración de resultados, mediante la triangulación de la información documental y los datos obtenidos, lo que permitió identificar riesgos críticos, niveles de cumplimiento normativo y áreas de mejora. Los datos cuantitativos fueron analizados mediante estadística descriptiva, utilizando frecuencias y porcentajes para representar la incidencia de riesgos y el grado de aplicación de medidas de seguridad. La información cualitativa fue analizada a través de análisis de contenido, permitiendo interpretar las relaciones entre normativa, prácticas organizacionales y riesgos emergentes. La investigación respetó principios éticos de confidencialidad y uso responsable de la información. Asimismo, se dejó constancia de que todos los materiales, instrumentos, criterios de evaluación y fuentes documentales utilizados en el estudio quedaron disponibles para su consulta, con el objetivo de que otros investigadores pudieran replicar o ampliar los resultados en contextos similares, conforme a las buenas prácticas de la investigación científica.

RESULTADOS Y DISCUSIÓN

Resultados sobre la seguridad integral y protección de infraestructuras

El análisis documental y contextual evidenció que la seguridad integral en la provincia de Santo Domingo de los Tsáchilas se encontró alineada, a nivel conceptual, con el enfoque establecido en la Constitución del Ecuador de 2008, el cual amplió la noción de seguridad desde una perspectiva estatal hacia una visión centrada en la protección del individuo, la organización y su entorno (Lucio Vásquez, 2020). No obstante, se identificaron brechas significativas entre el marco normativo y su aplicación práctica en la protección de infraestructuras.

Los principales resultados obtenidos fueron los siguientes:

• La protección de infraestructuras críticas presentó un enfoque predominantemente

ISSN: 3121-259X

reactivo, con escasa planificación preventiva frente a riesgos físicos y tecnológicos;

• Se evidenció una débil articulación entre los sistemas de gestión de riesgos y las políticas institucionales de seguridad integral;

• Las organizaciones analizadas priorizaron la continuidad operativa, pero sin incorporar de forma sistemática criterios de resiliencia y prevención multidimensional.

Estos resultados mostraron que, aunque el concepto de seguridad integral estuvo normativamente consolidado, su implementación operativa en el ámbito local fue fragmentada, coincidiendo con lo señalado por Lucio Vásquez (2020) respecto a la dificultad de traducir el paradigma de seguridad integral en prácticas institucionales consistentes.3.2. Resultados sobre seguridad laboral y riesgos ocupacionales. En relación con la seguridad y salud en el trabajo, los resultados reflejaron una alta exposición a riesgos laborales, particularmente en sectores caracterizados por condiciones de informalidad y limitada supervisión técnica. El análisis confirmó que las tasas de siniestralidad laboral y el subregistro de accidentes continuaron siendo problemáticas estructurales en el contexto ecuatoriano, con repercusiones visibles a nivel provincial (Gómez García, 2021).

De manera específica, se identificaron los siguientes hallazgos:

1. La implementación de sistemas de gestión de seguridad y salud en el trabajo fue heterogénea entre las organizaciones analizadas;
2. La cultura preventiva se encontró limitada, predominando acciones correctivas posteriores a la ocurrencia de incidentes;
3. La escasez de procesos sistemáticos de inspección y control influyó negativamente en el cumplimiento efectivo de la normativa vigente.

Estos resultados coincidieron con lo expuesto por Gómez García (2021), quien señaló que los cambios normativos y la reducción de mecanismos de auditoría habían impactado en la eficacia real de los sistemas de prevención de riesgos laborales en Ecuador.

Resultados sobre ciberseguridad y gestión de incidentes

El análisis de la dimensión de ciberseguridad evidenció que las organizaciones evaluadas presentaron niveles incipientes de madurez en la gestión de incidentes de seguridad de la información. Se observó que, si bien existieron controles tecnológicos básicos, estos no siempre estuvieron integrados en un modelo estructurado de respuesta ante incidentes.

Los resultados más relevantes fueron:

• La ausencia de metodologías formales para evaluar el nivel de madurez en la gestión de incidentes de ciberseguridad;

• La limitada capacitación del personal para la identificación, reporte y tratamiento de incidentes digitales;

• La dependencia de soluciones tecnológicas aisladas, sin una integración efectiva con

la gestión organizacional de riesgos.

Estos hallazgos se alinearon con lo descrito por Panche Abril et al. (2022), quienes demostraron que muchas organizaciones percibieron estar preparadas frente a incidentes cibernéticos, aunque en la práctica no contaban con procesos maduros ni evaluaciones sistemáticas que respaldaran dicha percepción.

Integración de resultados y enfoque multidimensional

La integración de los resultados de las tres dimensiones analizadas permitió identificar que la seguridad integral en la provincia de Santo Domingo de los Tsáchilas se desarrolló de manera fragmentada, sin una articulación efectiva entre la protección de infraestructuras, la seguridad laboral y la ciberseguridad. Se constató que los riesgos físicos, humanos y digitales fueron gestionados de forma independiente, lo que limitó la capacidad de respuesta ante amenazas complejas y multidimensionales. En conjunto, los resultados evidenciaron la necesidad de fortalecer modelos integrados de seguridad que consideren simultáneamente los entornos físico, laboral y digital, tal como lo sugiere el enfoque contemporáneo de seguridad integral aplicado al contexto ecuatoriano (Lucio Vásquez, 2020; Gómez García, 2021; Panche Abril et al., 2022).

DISCUSIÓN

Los resultados del estudio confirman que la seguridad integral, entendida como un enfoque multidimensional que articula la protección de infraestructuras, la seguridad laboral y la ciberseguridad, continúa presentando dificultades en su implementación práctica a nivel territorial. Aunque el marco normativo ecuatoriano reconoce la seguridad integral como un paradigma central de la política pública, los hallazgos evidencian que su aplicación en contextos provinciales, como Santo Domingo de los Tsáchilas, se desarrolla de manera fragmentada y con escasa integración operativa. Desde la perspectiva conceptual, los resultados se alinean con lo planteado por Lucio Vásquez (2020), quien sostiene que la transición desde la seguridad nacional hacia la seguridad integral implica no solo un cambio normativo, sino también una transformación institucional y cultural. En este sentido, el estudio muestra que dicha transformación aún se encuentra incompleta, ya que las organizaciones priorizan respuestas reactivas frente a amenazas específicas, sin consolidar modelos preventivos e integrados que contemplen simultáneamente riesgos físicos, humanos y digitales.

En relación con la seguridad laboral, los hallazgos refuerzan la evidencia presentada por Gómez García (2021), quien advierte que la existencia de normativa no garantiza, por sí sola, condiciones de trabajo seguras. La persistencia del subregistro de accidentes, la limitada cultura preventiva y la reducción de mecanismos de control e inspección continúan debilitando la efectividad de los sistemas de seguridad y salud en el trabajo. En este contexto, los resultados sugieren que la seguridad laboral sigue siendo abordada como un requisito formal,

ISSN: 3121-259X

más que como un componente estratégico de la seguridad integral.

Por su parte, la dimensión de ciberseguridad revela una brecha significativa entre la percepción de preparación organizacional y la madurez real en la gestión de incidentes. Esta situación coincide con lo expuesto por Panche Abril et al. (2022), quienes señalan que muchas organizaciones consideran que cuentan con capacidades suficientes para enfrentar incidentes cibernéticos, pese a no disponer de metodologías estructuradas ni evaluaciones sistemáticas de madurez. En consecuencia, la ciberseguridad se gestiona de forma aislada, sin integrarse plenamente a los sistemas de gestión de riesgos ni a la protección de infraestructuras críticas.

El alcance de los resultados permite comprender la seguridad integral como un fenómeno complejo, condicionado por factores normativos, organizacionales y culturales. No obstante, el estudio presenta limitaciones asociadas a su diseño transversal, ya que los datos reflejan una realidad contextualizada en un período específico y no permiten analizar la evolución temporal de los sistemas de seguridad. Asimismo, la investigación se centra en un ámbito provincial, lo que limita la generalización de los resultados a otras regiones del país con dinámicas productivas y sociales diferentes. A pesar de estas limitaciones, los hallazgos aportan evidencia relevante para el debate académico y práctico sobre la seguridad integral en contextos locales. Los resultados sugieren que futuras investigaciones deben profundizar en estudios longitudinales que evalúen la evolución de la seguridad integral en el tiempo, así como en el diseño y validación de modelos integrados que articulen infraestructura, trabajo y ciberseguridad. Asimismo, se considera pertinente ampliar el análisis comparativo entre provincias, con el fin de identificar buenas prácticas replicables y fortalecer la construcción de territorios más seguros y resilientes, en coherencia con el enfoque contemporáneo de seguridad integral en el Ecuador (Lucio Vásquez, 2020; Gómez García, 2021; Panche Abril et al., 2022).

Tabla 1.

Resultados sobre la protección de infraestructuras en el enfoque de seguridad integral en la provincia de Santo Domingo de los Tsáchilas

Dimensión evaluada	Aspecto analizado	Resultado observado	Interpretación del resultado
Protección de infraestructuras	Enfoque de gestión de la seguridad	Predominó un enfoque reactivo frente a incidentes y amenazas	La gestión se centró en la respuesta posterior al evento, con limitada planificación preventiva
Gestión de riesgos	Integración con políticas institucionales	Se identificó una débil articulación entre seguridad y planificación	La seguridad no se consolidó como eje transversal de la gestión organizacional

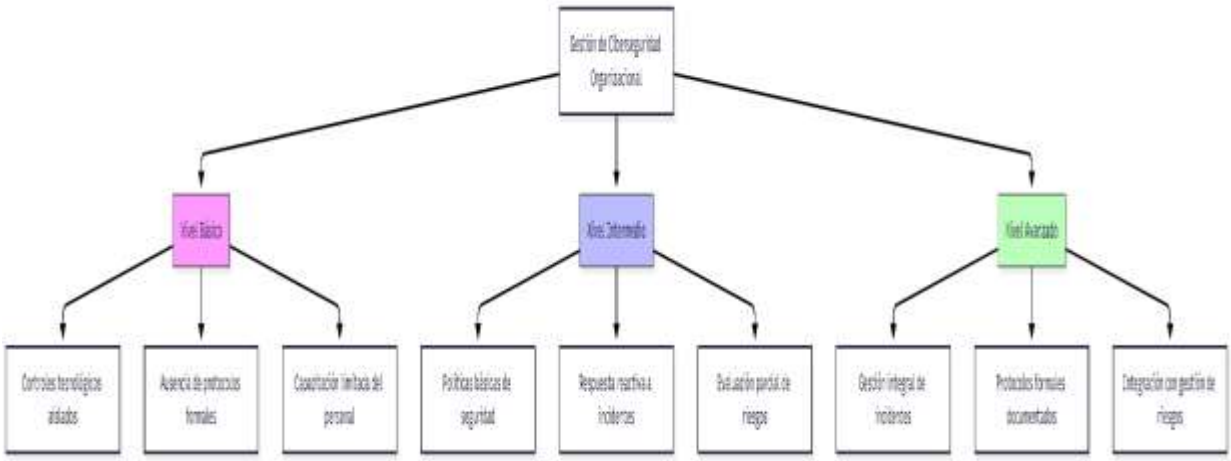
ISSN: 3121-259X

Dimensión evaluada	Aspecto analizado	Resultado observado	Interpretación del resultado
		estratégica	
Infraestructura crítica	Medidas de prevención física y tecnológica	Las medidas implementadas fueron parciales y no sistematizadas	Existió vulnerabilidad frente a riesgos físicos, operativos y tecnológicos
Continuidad operativa	Preparación ante eventos disruptivos	Se priorizó la continuidad operativa sin criterios formales de resiliencia	La infraestructura careció de planes integrales de recuperación y adaptación
Seguridad integral	Enfoque multidimensional	La seguridad se gestionó de forma fragmentada	No se evidenció integración efectiva entre infraestructura, trabajo y ciberseguridad

Nota. Los resultados se obtuvieron a partir del análisis documental y contextual de la seguridad integral en organizaciones públicas y privadas de la provincia de Santo Domingo de los Tsáchilas, considerando el marco normativo ecuatoriano y estudios previos sobre seguridad integral y protección de infraestructuras (Lucio Vásquez, 2020).

Figura 1

Nivel de madurez en la gestión de ciberseguridad en organizaciones de la provincia de Santo Domingo de los Tsáchilas.



Nota. La figura muestra los niveles de madurez identificados en la gestión de ciberseguridad organizacional (básico, intermedio y avanzado), considerando la existencia de controles tecnológicos, protocolos formales y su integración con la gestión de riesgos. La información se obtuvo a partir del análisis documental y contextual realizado en el estudio, y se interpretó en coherencia con enfoques de gestión de incidentes y madurez organizacional en ciberseguridad descritos en la literatura especializada (Panche Abril et al., 2022).

ISSN: 3121-259X

CONCLUSIONES

La investigación permitió demostrar que la seguridad integral, concebida como la articulación entre la protección de infraestructuras, la seguridad laboral y la ciberseguridad, aún no se consolida como un sistema integrado en el contexto provincial de Santo Domingo de los Tsáchilas. Los resultados evidencian que estas dimensiones continúan gestionándose de manera aislada, lo que limita la capacidad de las organizaciones para anticiparse y responder de forma efectiva a riesgos complejos y multidimensionales.

En relación con la protección de infraestructuras, el estudio confirma que la gestión de la seguridad se orienta principalmente hacia enfoques reactivos, priorizando la continuidad operativa inmediata antes que la prevención y la resiliencia. Esta situación implica que las infraestructuras físicas y tecnológicas permanecen expuestas a riesgos recurrentes, reduciendo su capacidad de adaptación frente a eventos disruptivos. De este modo, el objetivo de analizar la seguridad integral desde una perspectiva estructural se cumple al evidenciar la necesidad de fortalecer modelos preventivos y estratégicos en el ámbito local.

Respecto a la seguridad laboral, se concluye que, si bien existen marcos normativos y lineamientos formales, estos no se traducen de manera consistente en prácticas organizacionales sostenibles. La limitada cultura preventiva, la débil sistematización de los procesos de control y la persistencia de riesgos ocupacionales reflejan que la seguridad y salud en el trabajo no se integran plenamente como un componente estratégico de la seguridad integral. En este sentido, el estudio aporta evidencia sobre la brecha existente entre la normativa y su aplicación efectiva, lo que refuerza la necesidad de enfoques más articulados y contextualizados.

En el ámbito de la ciberseguridad, los hallazgos permiten concluir que las organizaciones presentan bajos niveles de madurez en la gestión de incidentes, caracterizados por la ausencia de metodologías formales, la capacitación limitada del personal y la dependencia de controles tecnológicos aislados. Esta realidad incrementa la vulnerabilidad institucional y compromete tanto la protección de la información como la seguridad de las infraestructuras críticas. El objetivo de identificar los principales desafíos en la ciberdefensa se alcanza al evidenciar que la dimensión digital continúa siendo subestimada dentro de los sistemas de gestión de seguridad.

De manera integral, la investigación aporta a la ciencia al proponer una lectura multidimensional de la seguridad aplicada a un contexto territorial específico, evidenciando cómo la fragmentación en la gestión de riesgos reduce la eficacia de las estrategias de protección. El estudio contribuye al debate académico al demostrar que la seguridad integral no puede abordarse de forma sectorial, sino que requiere modelos sistémicos que integren factores físicos, humanos y digitales.

ISSN: 3121-259X

Finalmente, se concluye que el principal aporte del trabajo radica en la generación de evidencia científica contextualizada para la provincia de Santo Domingo de los Tsáchilas, lo que permite visibilizar problemáticas locales desde un enfoque integral y replicable. Los objetivos planteados se consideran alcanzados al identificar brechas, desafíos y oportunidades de mejora, sentando bases para el diseño de políticas, estrategias organizacionales y futuras investigaciones orientadas a fortalecer la seguridad integral y la resiliencia territorial.

ISSN: 3121-259X

REFERENCIAS BIBLIOGRÁFICAS

Aguilar, L., & Salazar, M. (2019). Gestión integral de riesgos y seguridad organizacional en contextos latinoamericanos. Revista Latinoamericana de Seguridad, 6(2), 55–72.

Alexander, C. A., & Wang, L. (2024). Creación de un plan de ciberseguridad integrado para un sistema de salud. Revista Biomédica de Investigación Científica y Técnica, 56(5), Article 008926. https://doi.org/10.26717/BJSTR.2024.56.008926

Alvarado, P., & Molina, J. (2020). Infraestructuras críticas y resiliencia territorial: Un enfoque desde la gestión pública. Revista de Estudios Estratégicos, 12(1), 89–104.

Cruz, H., & Paredes, R. (2022). Ciberseguridad como componente de la seguridad integral en organizaciones públicas. Revista Iberoamericana de Sistemas de Información, 9(3), 61–77.

Gómez García, A. (2021). Seguridad y salud en el trabajo en Ecuador: Cambios normativos y siniestralidad laboral. Revista de Prevención de Riesgos Laborales, 4(2), 45–60. https://doi.org/10.32468/prl.v4i2.142

Hewage, C. (2021). Oportunidades, desafíos y estrategias para integrar la ciberseguridad y la seguridad en la práctica de la ingeniería. Revista de Acceso Abierto de Tecnología de Ingeniería,3(5), 555622. https://doi.org/10.19080/ETOAJ.2021.03.555622

Leroy, I., Zolotaryova, I., & Semenov, S. (2025). Impacto de la ciberseguridad de la infraestructura crítica en el desarrollo sostenible de las ciudades inteligentes: Perspectivas de especialistas internos y auditores externos de seguridad de la información. Sostenibilidad,17(3), 1188. https://doi.org/10.3390/su17031188

Lucio Vásquez, Á. A. (2020). La seguridad integral en el Ecuador: Alcances constitucionales y desafíos en su aplicación. Revista de Seguridad y Defensa, 8(1), 23–38. https://doi.org/10.37767/rsd.v8i1.43

Panche Abril, L. A., Ardila Gutiérrez, J. D., & Gutiérrez, M. A. (2022). Evaluación del nivel de madurez en la gestión de incidentes de ciberseguridad en organizaciones. Revista Iberoamericana de Sistemas y Tecnologías de la Información, (45), 89–104. https://doi.org/10.17013/risti.45.89-104

Rodríguez Zambrano, H. M., & Moreno Tamayo, C. H. (2024). Seguridad de la información y ciberseguridad: su importancia para los estados, empresas y las personas, una revisión sistemática. Estudios y Perspectivas Revista Científica y Académica, 4(1), 159–178. https://doi.org/10.61384/r.c.a..v4i1.90

Viteri Hernández, C., & Ávila, D. (2025). Exploración integral de la seguridad en redes de proveedores de servicios de internet: una revisión sistemática de literatura. Revista Perspectivas, 6(1), 215. https://doi.org/10.47187/perspectivas.6.1.215

Laszka, A., Abbas, W., Vorobeychik, Y., & Koutsoukos, X. (2018). Seguridad sinérgica para el Internet industrial de las cosas: Integración de redundancia, diversidad y fortalecimiento. Preimpresión en arXiv. https://arxiv.org/abs/1808.09090

Yigit, Y., Ferrag, M. A., Sarker, I. H., Maglaras, L. A., & Chrysoulas, C. (2024). Protección de infraestructuras críticas: IA generativa, desafíos y oportunidades. Preprint de arXiv. https://arxiv.org/abs/2405.04874

Ngobeni, H., & Nkongolo, M. W. (2025). Integrando la opinión pública y la experiencia técnica para una formulación efectiva de políticas de ciberseguridad. Preimpresión en arXiv. https://arxiv.org/abs/2512.08575