Ciencia Latina Revista Científica Multidisciplinar, Ciudad de México, México.
ISSN 2707-2207 / ISSN 2707-2215 (en línea), septiembre-octubre 2025,
Volumen 9, Número 5.

https://doi.org/10.37811/cl_rcm.v9i5

LAS ACTIVIDADES DE INTELIGENCIA PARA MITIGAR EL CIBERCRIMEN

INTELLIGENCE ACTIVITIES TO MITIGATE CYBERCRIME

Aldo Fernando Rejas de la Peña
Escuela de Posgrado PNP

Alex Celestino León Pacheco
Universidad Continental

Willian Andres Huarcaya Hilares
Escuela de Posgrado de la PNP

Giancarlos Veramendi Alhuay
Escuela de Posgrado de la PNP

DOI: https://doi.org/10.37811/cl_rcm.v9i5.20558

Las Actividades de Inteligencia para Mitigar el Cibercrimen

Aldo Fernando Rejas de la Peña[1]
43246299@escpograpnp.com
https://orcid.org/0000-0002-8594-8620
Escuela de Posgrado PNP

Alex Celestino León Pacheco
41867854@continental.edu.pe
https://orcid.org/0009-0009-7683-9367
Universidad Continental

Willian Andres Huarcaya Hilares
40292426@escpograpnp.com
https://orcid.org/0009-0006-8401-7687
Escuela de Posgrado de la PNP

Giancarlos Veramendi Alhuay
45274124@escpograpnp.com
https://orcid.org/0009-0000-8291-8701
Escuela de Posgrado de la PNP

RESUMEN

La presente investigación analizó cómo las actividades de inteligencia contribuyen a mitigar el cibercrimen, enmarcada en un estudio de tipo aplicado con un enfoque cualitativo y un diseño fenomenológico. Se contó con la participación de cuatro Analistas del máximo órgano rector de la inteligencia policial, quienes fueron seleccionados mediante por criterio de experto, dada su especialidad y experiencia directa en el campo. Para la recolección de datos se empleó la entrevista a profundidad como técnica y una guía semiestructurada como instrumento. Posteriormente, el procesamiento de la información cualitativa se realizó con el software ATLAS.ti, aplicando un sistema de codificación apriorística para el análisis sistemático de los hallazgos. Concluyendo que las actividades de inteligencia resultan cruciales en la mitigación del cibercrimen, pues permiten anticipar amenazas, desmantelar redes criminales y coordinar respuestas ante ataques globales. La integración de OSINT, SIGINT, la infiltración en entornos clandestinos y el análisis avanzado mediante inteligencia artificial fortalece la detección de actores maliciosos y vulnerabilidades. Además, la cooperación internacional y la retroalimentación interagencial fomentan estrategias ágiles y preventivas, consolidando la resiliencia institucional frente a escenarios criminales cada vez más sofisticados. Estos enfoques evidencian que la inteligencia es un pilar esencial para enfrentar los desafíos del panorama cibernético actual.

***Palabras claves*:** actividades de inteligencia, análisis, cibercrimen, difusión y recolección.

[1] Autor principal
Correspondencia: 43246299@escpograpnp.com

Intelligence Activities to Mitigate Cybercrime

ABSTRACT

This research analyzed how intelligence activities contribute to mitigating cybercrime, within the framework of an applied study with a qualitative approach and a phenomenological design. Four analysts from the highest governing body of police intelligence participated in the study. They were selected based on expert criteria, given their specialization and direct experience in the field. In-depth interviews were used as the data collection technique, and a semi-structured guide was used as the instrument. Subsequently, the qualitative information was processed using ATLAS.ti software, applying an a priori coding system for the systematic analysis of the findings. Concluding that intelligence activities are crucial in mitigating cybercrime, as they enable threats to be anticipated, criminal networks to be dismantled, and responses to global attacks to be coordinated. The integration of OSINT, SIGINT, infiltration into clandestine environments, and advanced analysis using artificial intelligence strengthens the detection of malicious actors and vulnerabilities. In addition, international cooperation and interagency feedback foster agile and preventive strategies, consolidating institutional resilience in the face of increasingly sophisticated criminal scenarios. These approaches demonstrate that intelligence is an essential pillar for addressing the challenges of today's cyber landscape.

***Keywords*:** intelligence, analysis, cybercrime, dissemination and collection activities.

Artículo recibido 02 setiembre 2025
Aceptado para publicación: 29 setiembre 2025

INTRODUCCIÓN

En el escenario global, las actividades de inteligencia desempeñan un papel fundamental en la lucha contra el cibercrimen. Según Bezzubov et al. (2017). la recolección de información a través de diversas fuentes, incluidas las redes sociales y los foros en línea, permite a los organismos internacionales identificar patrones y tendencias en el mundo digital. Asimismo, Holt & Bossler (2019) señalan que el análisis de esta información contribuye a la anticipación y mitigación de los ciberataques, facilitando la toma de decisiones estratégicas. Así también, destaca la importancia de la difusión efectiva de inteligencia entre las autoridades a nivel mundial, lo que fortalece la coordinación de esfuerzos y la implementación de medidas preventivas.

La creciente sofisticación de las amenazas cibernéticas ha impulsado a los países a desarrollar estrategias de inteligencia cibernética cada vez más robustas. Según Choo (2018), la recopilación de información a través de fuentes abiertas y cerradas es fundamental para comprender el modus operandi de los cibercriminales y anticipar sus movimientos. El análisis de inteligencia, como señalan Bada & Nurse (2019), juega un papel crucial en este proceso. A través del empleo de herramientas avanzadas de análisis de datos y machine learning, los analistas pueden identificar patrones sospechosos, predecir ataques inminentes y desarrollar estrategias proactivas para mitigar los riesgos cibernéticos. Las actividades de inteligencia desempeñan un papel fundamental en la prevención y mitigación de las amenazas digitales. La recolección de información proveniente de diversas fuentes permite a los organismos de inteligencia monitorear las actividades sospechosas en el ciberespacio y anticipar posibles ataques. Como señala Choo (2018), el análisis de esta información es crucial para identificar patrones y tendencias, lo que facilita la toma de decisiones estratégicas. Tounsi & Rais (2018) subrayan la importancia de la colaboración internacional en este ámbito. La difusión de inteligencia entre países y organizaciones es esencial para crear una defensa cibernética robusta y responder de manera coordinada y efectiva ante las amenazas transnacionales.

En el contexto latinoamericano, la inteligencia ha sido fundamental en la lucha contra el cibercrimen. Según Arce & Gómez (2020), la recolección de información a través de fuentes abiertas y encubiertas permite a los organismos de seguridad de la región entender la dinámica de las redes de ciberdelincuencia.

De igual manera, Rincón Arteaga et al. (2022) señalan que el análisis de esta información contribuye a la identificación de vulnerabilidades y amenazas específicas de la región, lo que facilita la implementación de medidas de prevención y mitigación. Asimismo, Solar (2023) destacan que la difusión de inteligencia entre los países latinoamericanos fortalece la cooperación y la coordinación de acciones para combatir el cibercrimen a nivel regional.

Las actividades de inteligencia han demostrado ser un pilar fundamental en la lucha contra el cibercrimen en Latinoamérica. Según Saavedra (2023), la recolección de información a través de diversas fuentes, como las redes sociales, permite a los organismos de seguridad anticipar y prevenir ataques cibernéticos. Sin embargo, Aguilar Antonio (2021) señalan que la región enfrenta desafíos significativos, como la falta de recursos y capacidades técnicas, que dificultan la implementación de estrategias de inteligencia efectivas.

La región latinoamericana enfrenta desafíos significativos en materia de ciberseguridad, como la falta de recursos y capacidades técnicas para llevar a cabo actividades de inteligencia efectivas. Según Henshaw (2024) muchos países carecen de infraestructuras adecuadas para el monitoreo y la recolección de datos, lo que los vuelve vulnerables a ciberataques. Sin embargo, iniciativas como el "Cybersecurity Capacity Building Programme", mencionado por Toapanta et al. (2020), han permitido fortalecer las habilidades de los profesionales de la región. La creación de redes de intercambio de información, como el "Cybersecurity Information Sharing Partnership" (Sarhan et al., 2023), ha facilitado la colaboración entre entidades y ha permitido a las fuerzas policiales desarrollar estrategias proactivas para anticipar y neutralizar las amenazas cibernéticas.

En el contexto peruano, las actividades de inteligencia han demostrado ser fundamentales para combatir el cibercrimen de manera efectiva. Vera (2023) destacan la importancia de la recolección de información a través de fuentes abiertas y encubiertas para identificar las particularidades de los ciberdelitos que afectan al país. Gutierrez et al. (2022) subrayan que el análisis de esta información permite diseñar estrategias de ciberseguridad más efectivas, adaptadas a la realidad nacional. Gracias a iniciativas como el "Cybersecurity Capacity Building Programme", mencionadas por Creese et al. (2021), los profesionales peruanos en ciberseguridad cuentan con las herramientas y conocimientos necesarios para identificar y mitigar las amenazas específicas que enfrenta el país.

La creación de redes de intercambio de información, como el "Cybersecurity Information Sharing Partnership", promovida por Piskors'ka et al. (2020), facilita la colaboración entre entidades peruanas y regionales, fortaleciendo así la respuesta ante incidentes cibernéticos.

La creciente sofisticación del cibercrimen ha impulsado la evolución de las actividades de inteligencia policial. Tal como señalan Gallardo Urbini (2020), la implementación de técnicas de recolección de datos provenientes de fuentes abiertas y cerradas ha permitido a las autoridades peruanas anticipar ciberataques y fortalecer sus capacidades de defensa. Esta proactividad, fundamental en un entorno digital en constante mutación, se complementa con el análisis de datos cibernéticos, el cual, según Del Pueblo (2023) revela patrones delictivos específicos que afectan al tejido social peruano.

La colaboración interinstitucional se ha posicionado como un pilar fundamental en esta lucha. Camille (2024) destacan la importancia de la difusión de inteligencia entre las diferentes agencias de seguridad para garantizar una respuesta coordinada y efectiva ante incidentes cibernéticos. La creación de redes de cooperación, al facilitar el intercambio de información y recursos, potencia la capacidad de respuesta del Estado ante las amenazas digitales. Finalmente, Bermudez Torres (2024) subraya la necesidad de una capacitación continua del personal involucrado en ciberseguridad, dado el dinamismo y la complejidad de las amenazas emergentes.

El cibercrimen representa una amenaza creciente para el desarrollo económico del Perú. Como señalan Antinori (2024), la inseguridad cibernética erosiona la confianza de los inversores y puede generar inestabilidad económica. Ante este escenario, las actividades de inteligencia policial adquieren una relevancia crucial. Al analizar incidentes cibernéticos y detectar patrones de amenaza, los organismos de seguridad pueden anticipar ataques y diseñar estrategias proactivas para proteger la infraestructura crítica y los activos digitales del país. Un marco legal sólido en ciberseguridad, como el propuesto por Montes (2020), es fundamental para respaldar estas iniciativas y garantizar la efectividad de las acciones de inteligencia.

Esta investigación explora la capacidad de las actividades de inteligencia para anticipar y neutralizar las amenazas cibernéticas. Al identificar proactivamente a los actores maliciosos y sus modus operandi, la inteligencia policial permite desarrollar estrategias preventivas y reactivas más efectivas.

El estudio se centra en la aplicación de técnicas de inteligencia para detectar y prevenir actividades ilícitas en el ciberespacio que atenten contra el bienestar de los usuarios de internet, considerando la naturaleza dinámica y evolutiva del cibercrimen.

De lo antes descrito en los párrafos anteriores se gesta el Problema general: ¿Cómo las actividades de inteligencia mitigan el cibercrimen?, así también los problemas específicos: ¿Cómo la recolección de información mitiga el cibercrimen?, ¿Cómo el análisis de información mitiga el cibercrimen?, y ¿Cómo la difusión de inteligencia mitiga el cibercrimen?

La Importancia de las actividades de inteligencia policial constituye un pilar fundamental en la investigación del cibercrimen, proporcionando información crucial sobre metodologías, redes y objetivos de los delincuentes digitales. Esta labor facilita la identificación de sospechosos, recopilación de evidencia digital y priorización de pistas prometedoras mediante herramientas especializadas que analizan datos provenientes de fuentes diversas como redes sociales, foros y la dark web.

En el ecosistema digital transfronterizo actual, estas actividades fomentan la colaboración internacional, permitiendo intercambiar información estratégica, anticipar ataques, implementar medidas preventivas y desarrollar respuestas globales coordinadas frente a amenazas cibernéticas en constante evolución.

El presente estudio constituye una herramienta esencial para profesionales de inteligencia policial que enfrentan la ciberdelincuencia. Mediante el análisis de actividades de inteligencia y su efectividad contra estos delitos, identificar mejores prácticas y áreas perfectibles. Ante la evolución constante de amenazas cibernéticas, aporta una base sólida para desarrollar nuevas metodologías investigativas que permitan la adaptación estratégica necesaria.

Por ende, se propone el *Objetivo de investigación*: Analizar cómo las actividades de inteligencia mitigan el cibercrimen, así también se presentan los *objetivos específicos*: Analizar cómo la recolección de información mitiga el cibercrimen, analizar cómo el análisis de información mitiga el cibercrimen y analizar cómo la difusión de inteligencia mitiga el cibercrimen.

Actividades de inteligencia

Conforme al Manual de doctrina de inteligencia policial (2022), las actividades de inteligencia son acciones sistemáticas de recolección, análisis y difusión de inteligencia sobre amenazas y vulnerabilidades. Este ciclo integra fuentes abiertas (OSINT) y cerradas para generar conocimiento estratégico, facilitando la toma de decisiones para la prevención y neutralización de riesgos. Su finalidad es proteger la seguridad pública, la defensa nacional y las infraestructuras críticas, consolidándose como una herramienta fundamental para la protección y gobernanza del Estado.

La inteligencia policial se centra en la prevención delictiva a través del análisis riguroso de información. Hughes (2023) la concibe como la identificación de patrones para crear estrategias preventivas, mientras que Carter (2013) subraya su indispensable carácter proactivo. Esta labor se fortalece con la colaboración interagencial, como destaca Wang et al. (2019). Además, se nutre de análisis especializados de redes sociales, valorado por Yang et al. (2016), y del análisis espacial para comprender la geografía del delito, como resaltan Chainey & Ratcliffe (2013).

Las actividades de inteligencia policial exigen un estricto marco ético y el pleno respeto a los derechos humanos. Sarkar et al. (2023) subraya la necesidad de transparencia, rendición de cuentas y confidencialidad. Por su parte, O'Malley (2016) destaca la importancia de orientar estas acciones a satisfacer las necesidades de la comunidad. Para prevenir abusos y garantizar la legitimidad de las operaciones, Heikkila & Kunelius (2020) consideran indispensable la implementación de mecanismos robustos de regulación y supervisión constante.

Recolección de información: es un pilar fundamental del ciclo de inteligencia ya que proporciona los insumos esenciales para la toma de decisiones estratégicas. El Manual de Doctrina de Inteligencia Policial (2022) destaca la importancia de diversificar las fuentes, combinando medios abiertos y encubiertos para asegurar datos precisos.

En esa línea, la Policía Nacional de Colombia (2022) establece que los agentes deben dominar la identificación y evaluación de fuentes, mientras que las operaciones de vigilancia y seguimiento encubierto son cruciales para obtener información de primera mano y consolidar el conocimiento sobre las amenazas.

Análisis de información: es el proceso sistemático de examinar datos para extraer conclusiones que orienten la toma de decisiones. Según el Manual de doctrina de inteligencia policial (2022), esta labor es crucial para identificar patrones y tendencias en fenómenos complejos. La correcta aplicación de las metodologías, como enfatizan Cinelli & Gran (2019), mejora la capacidad de respuesta institucional. En última instancia, un análisis riguroso resulta fundamental para formular estrategias efectivas en la prevención del delito y optimizar los recursos, tal como lo señalan Feng et al. (2019), consolidando así la base del conocimiento estratégico.

Difusión de inteligencia: constituye la fase estratégica destinada a entregar el producto de inteligencia a los usuarios autorizados a través de canales seguros y oportunos, garantizando su pertinencia y reserva legal (Manual de Doctrina de Inteligencia Policial, 2022). Este proceso asegura que los hallazgos sean aprovechados eficazmente en la toma de decisiones y en la prevención de riesgos. Su efectividad depende de la elección de medios adecuados de transmisión (Villamizar Moreno & Pedraza Uribe, 2023), así como de la claridad comunicativa para evitar interpretaciones erróneas (Arab & Muneeb, 2019). De esta manera, la difusión fortalece la coordinación interinstitucional y optimiza la respuesta de las fuerzas del orden.

Cibercrimen

Esta nueva amenaza engloba delitos ejecutados mediante tecnologías digitales, representando una grave amenaza global cuyo crecimiento exponencial es advertido por Rendón et al. (2024). Su complejidad no solo radica en la constante evolución táctica, sino en la capacidad de los delincuentes para instrumentalizar la innovación a su favor. Como señala Alghamdi (2020), esta ventaja tecnológica les permite eludir sistemas defensivos cada vez más sofisticados, manteniendo una asimetría estratégica en el ciberespacio y dificultando los esfuerzos de prevención y respuesta por parte de las autoridades competentes.

Dada su naturaleza transnacional, la lucha contra el cibercrimen exige ineludiblemente un enfoque global y coordinado. Castillo Pulido & Jiménez Acosta (2024) subrayan que la colaboración internacional y el intercambio ágil de inteligencia son los pilares para articular respuestas efectivas contra estas redes delictivas.

Este desafío multifacético demanda no solo una actualización constante de las estrategias de ciberseguridad, sino también una cooperación reforzada y sin fisuras entre agencias globales. Se trata de la única vía posible para lograr un control y una prevención eficaces frente a una amenaza en perpetua mutación.

MÉTODO

Tipo de investigación, enfoque y diseño

La presente investigación se enmarca en un tipo aplicado**,** considerado esencial para el avance del conocimiento y la generación de soluciones efectivas a problemáticas reales. Según Gregar (2023), este tipo de investigación transforma de manera significativa nuestra comprensión del mundo al vincular teoría y práctica, mientras que Babbie (2020) resalta su función en el desarrollo de aplicaciones concretas orientadas a la solución de necesidades sociales. Por su parte, Hernández-Sampieri y Mendoza (2018) destacan su impacto en la creación de innovaciones tecnológicas, y Mertens (2020) subraya su potencial para estimular la creatividad frente a los desafíos globales.

El enfoque cualitativo de investigación examina en profundidad los significados y vivencias humanas en sus contextos naturales. Su objetivo es fomentar la construcción conjunta de conocimiento, como señalan Ñaupas et al. (2023), y desarrollar teorías genuinas, según Gregar (2023). Para lograrlo, la reflexividad del investigador es esencial en la identificación de sesgos, como enfatiza Flick (2022); un principio que Kuckartz & Radiker (2023) consideran crucial para captar la riqueza de la experiencia humana sin caer en simplificaciones.

El diseño fenomenológico es una herramienta poderosa para generar conocimiento profundo sobre fenómenos complejos. Según Hernández-Sampieri & Mendoza (2018), este enfoque explora las dimensiones subjetivas de la experiencia humana para revelar significados ocultos. Dicha comprensión tiene aplicaciones prácticas, pues como enfatizan Ñaupas et al. (2023), facilita el desarrollo de programas más sensibles a las necesidades de los participantes. A su vez, al iluminar diversas vivencias, este diseño promueve el diálogo entre grupos sociales, contribuyendo a una sociedad más justa, como lo sugiere Brown (2021).

Participantes

Son los actores centrales que proporcionan la información esencial, por lo que su selección es un proceso deliberado y crucial. Como señalan Ñaupas et al. (2023), dicha selección debe ser guiada por los objetivos del estudio para comprender a fondo el fenómeno. Acorde con este principio, se optó por un muestreo de expertos cualificados, decisión metodológica que se alinea con Sánchez (2018) y García & López (2023). Estos autores sostienen que dicho enfoque es indispensable para obtener una perspectiva profunda y enriquecer el análisis con conocimiento teórico-práctico invaluable.

Con base en este marco, se contó con la colaboración de cuatro Analistas del máximo órgano rector de la inteligencia policial. Para garantizar su idoneidad, los criterios de inclusión fueron rigurosos: ser especialista calificado en inteligencia, acreditar una experiencia mínima de diez años en la comunidad y poseer certificación vigente en operaciones contra el cibercrimen. El cumplimiento de estos requisitos aseguró una visión interna y sustantiva del tema. Por consiguiente, el criterio de exclusión se aplicó a todo personal que, aun perteneciendo al sistema de inteligencia, no demostrara la pericia específica requerida.

Técnicas e instrumentos de recolección de datos

La entrevista, como técnica cualitativa, es un proceso de co-construcción del conocimiento. Ñaupas et al. (2023) y Gregar (2023) destacan que la interacción entre entrevistador y entrevistado permite explorar en profundidad las experiencias de los participantes. Esta flexibilidad facilita la adaptación de preguntas, enriqueciendo la comprensión del fenómeno estudiado. Rojas-Gutiérrez (2022) resaltan su utilidad para temas complejos, mientras Neale (2021) enfatizan las habilidades del entrevistador. Como instrumento *La guía de entrevista*, según Hernández-Sampieri y Mendoza (2018), es fundamental para estructurar la recolección de datos, permitiendo explorar aspectos inesperados y garantizando la validez y confiabilidad de los resultados.

Una vez validados los instrumentos por juicio de expertos, se procedió con la recolección de datos, obteniendo primero el consentimiento informado de los cuatro analistas de inteligencia participantes. Dada la naturaleza sensible de la investigación, se realizaron entrevistas a profundidad de manera presencial, en un entorno seguro y propicio coordinado según la disponibilidad de cada experto para garantizar la máxima confianza y franqueza.

Durante estas sesiones, los analistas aportaron su valiosa experiencia en relación con el objeto de estudio. Para salvaguardar la confidencialidad y el rigor ético del proceso, cada fuente fue anonimizada mediante la codificación EE1, EE2, EE3 y EE4.

Para el procesamiento de los datos cualitativos, se empleó un enfoque sistemático utilizando el software ATLAS.ti. Las transcripciones completas de las entrevistas a profundidad fueron importadas a esta plataforma, donde se aplicó un marco de codificación a priori, diseñado específicamente para estructurar el análisis sobre cómo las actividades de inteligencia mitigan el cibercrimen. Este análisis cualitativo permitió generar diversas representaciones visuales; incluyendo nubes de palabras, diagramas de Sankey y gráficos de redes.

Con el fin de identificar patrones, jerarquías y conexiones relevantes en el discurso de los expertos. Dichas visualizaciones elaboradas constituyeron un recurso esencial, pues no solo facilitaron la interpretación detallada de los resultados, sino que también permitieron comunicar la evidencia empírica de forma clara y precisa, aportando solidez al análisis e incrementando la comprensión del fenómeno investigado (Rejas de la Peña et al., 2025).

RESULTADOS

Los resultados obtenidos de las entrevistas a cuatro analistas del ente rector de inteligencia policial, especializados en la mitigación del cibercrimen, permitieron identificar acciones orientadas al fortalecimiento de estrategias operativas frente a estas nuevas tendencias delictivas. Como expertos en patrullaje virtual, su aporte resultó fundamental para consolidar la ciberseguridad en un entorno marcado por amenazas crecientes y diversas modalidades de ciberdelito. La información recogida fortaleció significativamente esta investigación, y mediante el análisis con el software ATLAS.ti, se presentaron resultados gráficos que evidencian los hallazgos para optimizar estrategias policiales en la lucha contra el ciber crimen.

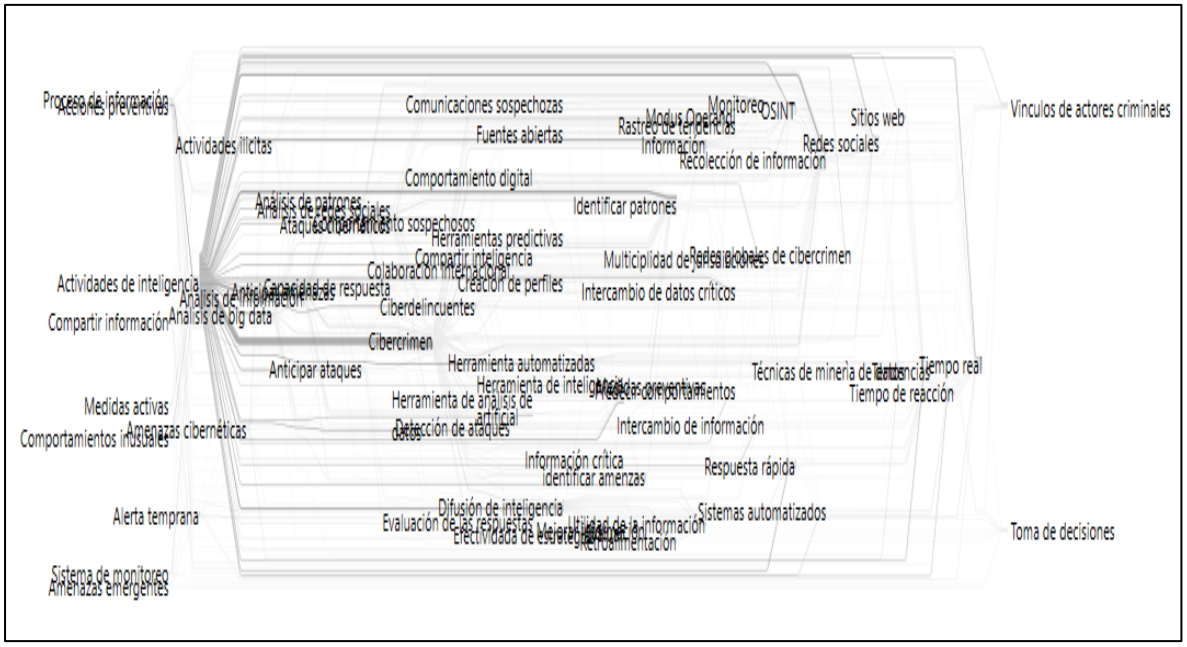
Figura 1 Nube de palabras

Nota: datos obtenidos del análisis de las entrevistas en el Software ATLAS.ti.

El análisis de la nube de palabras resalta que la información, el análisis y la inteligencia son los conceptos centrales. Estos elementos permiten procesar datos y volúmenes de información para identificar patrones y tendencias de amenazas y ataques cibernéticos. Palabras como herramientas, agencias, colaboración y OSINT (Open Source Intelligence) sugieren que esta labor se lleva a cabo mediante el uso de tecnologías especializadas y un esfuerzo conjunto. El objetivo es claro: detectar y mitigar el cibercrimen, lo que se logra al obtener una respuesta rápida y efectiva frente a las actividades criminales. Esto indica que el foco principal está en la aplicación práctica de la inteligencia para la seguridad cibernética.

El análisis realizado muestra que la inteligencia desempeña un papel esencial en la mitigación del cibercrimen, ya que implica procesar grandes volúmenes de información y datos a través de análisis sistemáticos y herramientas especializadas. Los conceptos de información, análisis y colaboración emergen como centrales, indicando que tanto las agencias como la utilización de OSINT y tecnologías avanzadas resultan fundamentales para identificar patrones y tendencias de amenazas cibernéticas. Se observa que la coordinación entre diferentes actores fortalece la capacidad de respuesta rápida y efectiva, asegurando que la inteligencia no solo aporte conocimiento, sino que habilite acciones concretas para prevenir y contrarrestar el cibercrimen de manera proactiva y eficiente.

Figura 2 Diagrama de Sankey

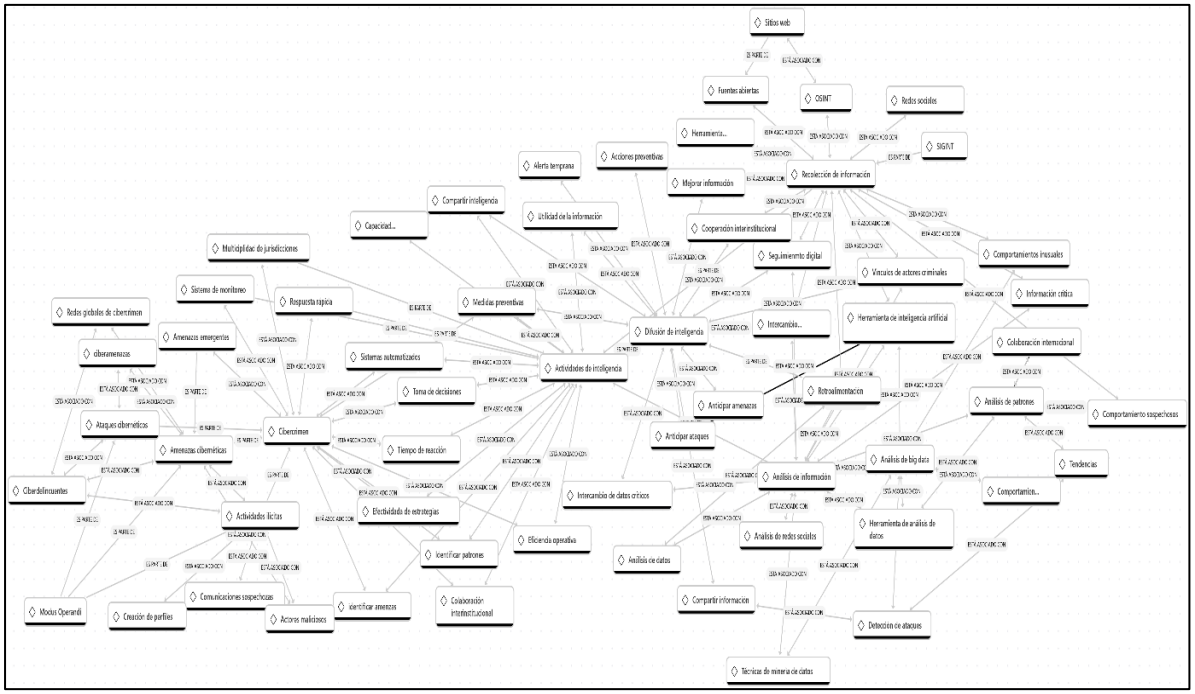


Nota: datos obtenidos del análisis de las entrevistas en el Software ATLAS.ti

El diagrama de Sankey ilustra el flujo de cómo las actividades de inteligencia y el análisis de información de fuentes como OSINT y redes sociales, permiten mitigar el cibercrimen. Muestra que la recolección de datos y la evaluación de amenazas emergentes son cruciales para identificar patrones y comportamientos sospechosos. Este proceso, apoyado por la colaboración entre agencias y el uso de herramientas automatizadas, facilita la detección de ataques y una respuesta rápida. En última instancia, todo este flujo de información y análisis culmina en una efectiva toma de decisiones, con el fin de desarticular los vínculos de actores criminales y mejorar el tiempo de reacción ante nuevas amenazas.

Este diagrama, evidencia que las actividades de inteligencia resultan fundamentales para mitigar el cibercrimen, ya que representan un proceso dinámico y colaborativo en la gestión de amenazas. La recolección y el análisis de información desde fuentes abiertas como OSINT y redes sociales, junto con herramientas automatizadas, posibilitan identificar patrones y detectar comportamientos sospechosos en tiempo real. La colaboración interagencial refuerza la capacidad para responder rápidamente y optimizar la toma de decisiones, permitiendo desarticular redes criminales y mejorar la reacción ante nuevas amenazas, alineando así las acciones de inteligencia con la seguridad cibernética.

Figura 3 Diagrama de Redes



Nota: datos obtenidos del análisis de las entrevistas en el Software ATLAS.ti.

El diagrama de redes ilustra las actividades de inteligencia como el eje central para la lucha contra el cibercrimen. Muestra que la recolección de información de fuentes abiertas alimenta un proceso de análisis de inteligencia para identificar patrones y vínculos de actores criminales. Este proceso es apoyado por sistemas automatizados, permitiendo la detección de amenazas y un monitoreo constante. La colaboración internacional y el intercambio de información son cruciales para obtener una visión global. El objetivo final es informar la toma de decisiones para lograr una respuesta rápida y mitigar los riesgos, demostrando un ciclo integral desde la obtención de datos hasta la acción efectiva.

El diagrama de redes demuestra que las actividades de inteligencia son esenciales para mitigar el cibercrimen, pues integran la recolección de datos desde fuentes abiertas y el análisis automatizado para identificar patrones delictivos. Sistemas tecnológicos avanzados favorecen la detección de amenazas y el monitoreo constante, permitiendo anticipar riesgos y reducir el impacto de ataques. La colaboración internacional y el intercambio de información otorgan una perspectiva global, mejorando la capacidad de reacción ante incidentes. Así, la toma de decisiones se fundamenta en información precisa, posibilitando una respuesta eficiente y efectiva para combatir el cibercrimen desde la inteligencia integral.

Después del análisis interpretativo de los datos obtenidos mediante el software ATLAS.ti, se realizó la contrastación sistemática de las entrevistas, con el fin de garantizar la validez y coherencia del estudio. Este proceso permitió identificar de manera rigurosa las coincidencias y discrepancias en los discursos de los participantes, siempre en relación con los objetivos planteados en la investigación. De este modo, se estableció un marco sólido para la exposición de los hallazgos, los cuales se detallan a continuación.

Objetivo de investigación: Analizar cómo las actividades de inteligencia mitigan el cibercrimen.

Los entrevistados (EE1, EE2, EE3 y EE4) coinciden de manera categórica en que las actividades de inteligencia resultan esenciales para mitigar el cibercrimen, ya que permiten anticipar conductas delictivas y desarticular estructuras criminales antes de que logren materializar ataques de mayor impacto. Todos destacan la importancia del uso de OSINT y la vigilancia en redes abiertas y clandestinas como la dark web, que, sumadas a técnicas de infiltración y operaciones encubiertas, facilitan identificar actores, modus operandi y trazabilidad de transacciones ilícitas. Asimismo, señalan la relevancia del análisis automatizado de grandes volúmenes de datos mediante inteligencia artificial y machine learning, herramientas que ofrecen un panorama integral y predictivo. De igual manera, resaltan que la cooperación internacional y el intercambio de inteligencia fortalecen la capacidad para enfrentar amenazas transnacionales, consolidando estrategias policiales más ágiles y efectivas.

Los especialistas (EE1, EE2, EE3 y EE4), si bien comparten la premisa de que la inteligencia es indispensable para enfrentar el cibercrimen, difieren en cuanto a los énfasis y enfoques metodológicos. EE1 sostiene que el monitoreo de la deep web y foros clandestinos es prioritario, mientras EE2 pondera el análisis predictivo de patrones comportamentales como la vía más efectiva para la prevención. EE3, en cambio, otorga mayor valor a los sistemas SIEM y a la correlación de eventos en tiempo real, mientras que EE4 plantea que el uso de SIGINT y el rastreo de criptomonedas resultan clave para descubrir redes de financiamiento criminal. Estas discrepancias reflejan que, aunque existe consenso en la necesidad de inteligencia integral, las prioridades operativas y las herramientas consideradas más útiles varían según la experiencia y especialidad de cada analista.

Objetivo Específico 1: Analizar cómo la recolección de información mitiga el cibercrimen.

Los especialistas coinciden en que la recolección de información, tanto de fuentes abiertas (OSINT) como de fuentes cerradas y operaciones encubiertas, es un elemento crucial para mitigar el cibercrimen. EE1, EE2, EE3 y EE4 resaltan que técnicas como el monitoreo de redes sociales, foros clandestinos, la observación de la deep y dark web, y el uso de herramientas de análisis de tráfico digital permiten anticipar amenazas, identificar a actores maliciosos y rastrear sus métodos. Además, señalan que OSINT constituye una herramienta clave por su accesibilidad, legalidad y bajo costo, facilitando el análisis preventivo y la toma de decisiones rápidas. De igual forma, los expertos coinciden en la importancia de la colaboración internacional, afirmando que el cibercrimen es transnacional y requiere del intercambio coordinado de datos para identificar patrones globales y neutralizar redes delictivas a gran escala, reforzando así la capacidad de reacción preventiva sobre escenarios de riesgo.

Los entrevistados muestran diferencias en la priorización de técnicas y enfoques frente a la recolección de información para mitigar el cibercrimen. EE1 enfatiza la infiltración en foros clandestinos y el uso de datos confidenciales con agentes encubiertos, mientras que EE2 privilegia las técnicas de minería de datos y la identificación de patrones de comportamiento en línea. En contraste, EE3 otorga mayor relevancia a honeypots y vigilancia electrónica, mientras EE4 integra OSINT con SIGINT como componentes complementarios y críticos para interceptar comunicaciones. Sobre la recolección de OSINT, EE1 resalta la detección temprana de tendencias, mientras EE3 enfatiza las ventajas de bajo costo y marco legal. Finalmente, aunque todos valoran la colaboración internacional, EE1 hace hincapié en el acceso a información restringida mediante acuerdos formales, mientras EE2 y EE4 ponen mayor peso en la anticipación de amenazas a través del intercambio inmediato de inteligencia. Estas diferencias reflejan la diversidad de metodologías, aun dentro de un objetivo común.

Objetivo Específico 2: Analizar cómo el análisis de información mitiga el cibercrimen.

Los especialistas coinciden en que el análisis de información es fundamental para mitigar el cibercrimen, debido a que permite anticipar amenazas, correlacionar datos y detectar patrones de comportamiento sospechosos en entornos complejos. EE1, EE2, EE3 y EE4 destacan que

herramientas como inteligencia artificial, machine learning y plataformas de análisis de datos (Maltego, Palantir, Splunk, SIEM) resultan esenciales para procesar grandes volúmenes de información, identificar anomalías y mapear relaciones entre actores criminales. Asimismo, subrayan que el big data es clave al proporcionar una visión holística de las amenazas y facilitar la detección de ataques avanzados, como APT. Para todos, el análisis de información posibilita predecir ciberataques mediante la observación de patrones recurrentes, indicadores tempranos de compromiso y vulnerabilidades explotadas anteriormente, lo que otorga ventajas significativas en la acción preventiva y la protección proactiva de infraestructuras críticas.

Los entrevistados presentan diferencias en la jerarquización de las herramientas y metodologías más eficaces para el análisis contra el cibercrimen. EE1 resalta la combinación de inteligencia artificial, forense digital, big data y SIEM como piezas centrales para anticipar ataques; mientras que EE2 se concentra especialmente en el valor de la correlación de datos históricos para identificar repeticiones y comportamientos sospechosos sin profundizar en soluciones altamente especializadas. EE3 enfatiza el uso de indicadores de compromiso (IOC) y la correlación de información en tiempo real como mecanismo predictivo, diferenciándose de EE4, quien prioriza el empleo de inteligencia artificial predictiva para generar alertas anticipadas. Respecto al big data, EE1 lo proyecta como indispensable para descubrir amenazas avanzadas, frente a EE2 que lo concibe más como herramienta de priorización de riesgos. Estas discrepancias reflejan un mismo objetivo, pero con enfoques técnicos diferenciados según la experiencia y perspectiva de cada especialista.

Objetivo Específico 3: Analizar cómo la difusión de inteligencia mitiga el cibercrimen.

Los especialistas coinciden en que la difusión de inteligencia es un factor esencial para mitigar el cibercrimen, ya que fortalece la coordinación interinstitucional, garantiza una respuesta más rápida y evita que existan vacíos de comunicación explotados por los delincuentes. EE1, EE2, EE3 y EE4 resaltan que la difusión entre agencias permite compartir datos en tiempo real sobre actores, tácticas y vulnerabilidades, asegurando que las contramedidas sean coherentes y sincronizadas. Asimismo, todos destacan la utilidad de mecanismos como sistemas de alerta temprana, plataformas seguras de intercambio de información (ISACs), boletines de inteligencia y notificaciones automatizadas, que permiten anticiparse a amenazas emergentes.

También hay consenso en que la retroalimentación es vital, pues posibilita ajustar procesos, afinar protocolos de comunicación y garantizar que la inteligencia compartida sea pertinente, clara y efectiva, reforzando la prevención y la capacidad de respuesta integrada.

Los especialistas entrevistados destacan distintos enfoques sobre mecanismos de difusión y retroalimentación. EE1 prioriza sistemas automatizados de alerta basados en inteligencia artificial, reforzando con reuniones periódicas e informes; EE2 privilegia alertas en tiempo real y reportes de tendencias. EE3 resalta el valor de los SIEM y boletines como herramientas clave, mientras EE4 considera esencial la certificación de alerta temprana y las redes ISAC en la colaboración interagencial. Respecto a la retroalimentación, EE1 busca optimizar protocolos y la interpretación de datos, EE2 ajusta la relevancia de los mensajes, EE3 promueve una mayor cooperación y EE4 trabaja para mejorar la claridad y pertinencia de las alertas. Estas diferencias reflejan enfoques complementarios, vinculados directamente con las prácticas operativas y la experiencia individual de cada especialista.

CONCLUSIONES

Primera: Las actividades de inteligencia resultan cruciales en la mitigación del cibercrimen, pues permiten anticipar amenazas, desmantelar redes criminales y coordinar respuestas ante ataques globales. La integración de OSINT, SIGINT, la infiltración en entornos clandestinos y el análisis avanzado mediante inteligencia artificial fortalece la detección de actores maliciosos y vulnerabilidades. Además, la cooperación internacional y la retroalimentación interagencial fomentan estrategias ágiles y preventivas, consolidando la resiliencia institucional frente a escenarios criminales cada vez más sofisticados. Estos enfoques evidencian que la inteligencia es un pilar esencial para enfrentar los desafíos del panorama cibernético actual.

Segunda: La recolección de información se consolida como el eje fundamental para mitigar el cibercrimen, al permitir identificar actores, detectar patrones de comportamiento y anticipar amenazas antes de su ejecución. El uso de OSINT, SIGINT, infiltraciones en foros clandestinos, honeypots y análisis de tráfico digital otorgan a las agencias de inteligencia capacidades preventivas y de rastreo que fortalecen la acción operativa.

Asimismo, la cooperación internacional y el intercambio ágil de datos resultan determinantes para enfrentar la naturaleza transnacional del cibercrimen, optimizando la reacción preventiva y la protección integral.

Tercera: El análisis de información se constituye como un pilar estratégico para mitigar el cibercrimen, ya que permite anticipar ataques, correlacionar datos y descubrir patrones sospechosos que fortalecen la acción preventiva. El uso de inteligencia artificial machine learning, big data y plataformas como SIEM o Palantir optimiza la detección de anomalías y la comprensión de conexiones entre actores criminales. Esta capacidad analítica brinda una visión integral que posibilita identificar indicadores tempranos de compromiso, detectar amenazas avanzadas y proteger infraestructuras críticas con mayor eficacia y proactividad.

Cuarta: La difusión de inteligencia constituye un recurso estratégico para mitigar el cibercrimen, dado que potencia la coordinación interinstitucional, reduce los tiempos de reacción y evita que los delincuentes se aprovechen de vacíos de comunicación. El intercambio oportuno de datos sobre actores, tácticas y vulnerabilidades, a través de sistemas de alerta temprana, redes seguras ISACs y boletines especializados, asegura contramedidas coherentes y sincronizadas. Asimismo, la retroalimentación continua optimiza los procesos de comunicación, garantizando que la inteligencia compartida sea clara, pertinente y efectiva en la prevención.

REFERENCIAS BIBLIOGRAFICAS

Aguilar Antonio, J. M. (2021). Retos y oportunidades en materia de ciberseguridad de América Latina frente al contexto global de ciberamenazas a la seguridad nacional y política exterior. *Estudios internacionales (Santiago)*, *53*(198), 169-197.Arroyo, C. (2006). Los Desafíos de la Inteligencia Regional en un Contexto de Globalización.

Alghamdi, M. I. (2020). A descriptive study on the impact of cybercrime and possible measures to curtail its spread worldwide. International Journal of Engineering Research and Technology, 9(731), 35.

Antinori, V. H. C. L. (2024). Influencia de los Delitos Cibernéticos Económicos en Perú. SCIÉNDO, 27(4), 415-418.

Arab, Z., & Muneeb, A. (2019). An employees' perspective of effective communication as a strategy for enhancing organizational performance. *Management*, *2*(1), 104-122.

Bada, M., & Nurse, J. R. C. (2019). The Social and Psychological Impact of Cyber-Attacks. Oxford University Press.

Baker, L., Phelan, S., Snelgrove, R., Varpio, L., Maggi, J., & Ng, S. (2016). Recognizing and responding to ethically important moments in qualitative research. Journal of Graduate Medical Education, 8(4), 607-608.

Bermudez Torres, M. A. (2024). Aplicación de estándares de ciberseguridad para proteger la información de las organizaciones.

Bezzubov, D., Ihonin, R., & Diorditsa, I. (2017). Cyberthreats as a component of threats in the contemporary world (a legal aspect). Journal of Advanced Research in Law and Economics, 8(7 (29)), 2086-2093.

Brown, M. (2021). Truth and method in southern criminology. Critical Criminology, 29(3), 451-467.

Camille, V. (2024). La cooperación para la investigación y persecución penal del Crimen Organizado Transnacional en Bolivia, Perú, Chile y Argentina.

Carter, D. L. (2013). Law enforcement intelligence: A guide for state, local, and tribal law enforcement agencies. Office of Community Oriented Policing Services.

Castillo Pulido, L. E., & Jiménez Acosta, J. F. (2024). Cooperación internacional policial ante amenazas cibernéticas en Colombia: Modalidad Business Email Compromise. *Revista Logos Ciencia & Tecnología*, *16*(1), 83-107.

Cinelli, V., & Gan, A. M. (2019). El uso de programas de análisis predictivo en la inteligencia policial: una comparativa europea. Revista de estudios en seguridad internacional, 5(2), 1-19.

Chainey, S., & Ratcliffe, J. H. (2013). GIS and crime mapping. John Wiley & Sons.

Choo, K. K. R. (2018). Cyber threat landscape faced by financial and insurance industry. Trends and Issues in Crime and Criminal Justice, 456, 1-11.

Creese, S., Dutton, W. H., Esteve-Gonzalez, P., & Shillair, R. (2021). Cybersecurity capacity-building: cross-national benefits and international divides. Journal of Cyber Policy, 6(2), 214-235.

Del Pueblo, D. (2023). La ciberdelincuencia en el Perú: estrategias y retos del Estado. Recuperado el, 14.

Dirección Nacional de Inteligencia. (2022). Sistema de Inteligencia Nacional (SINA). Recuperado de https://www.gob.pe/direccion-nacional-de-inteligencia

Feng, M., Zheng, J., Ren, J., Hussain, A., Li, X., Xi, Y., & Liu, Q. (2019). Big data analytics and mining for effective visualization and trends forecasting of crime data. IEEE Access, 7, 106111-106123.

Flick, U. (2022). The SAGE handbook of qualitative research design.

Gallardo Urbini, I. M. (2022). Estrategia de Ciberseguridad Distribuida, aplicando el concepto de Operación de Inteligencia (Doctoral dissertation, Universidad Nacional de La Plata).

Gregar, J. (2023). Research design (qualitative, quantitative and mixed methods approaches). Research Design, 8.

Gutierrez, E. D. L., Gomez, C. M. T., Arcaya, Y. A. E., & Montoya, L. A. G. (2022). Revisión de los avances y cambios en ciberseguridad en el Perú, para una transformación digital. Innovation and Software, 3(2), 109-120.

Heikkilä, H., & Kunelius, R. (2020). Surveillance and the structural transformation of privacy: Mapping the conceptual landscape of journalism in the post-Snowden era. In Journalism, Citizenship and Surveillance Society (pp. 7-21). Routledge.

Henshaw, A. (2024). Capacity Building and Cyber Insecurity in Latin America. Critical Perspectives on Cybersecurity: Feminist and Postcolonial Interventions, 173.

Hernández Samperio, J., & Mendoza, J. (2018). Métodos de investigación en ciencias sociales. Editorial Académica.

Holt, T. J., & Bossler, A. M. (2019). The Palgrave handbook of international cybercrime and cyberdeviance. Palgrave Macmillan.

Hughes, C. (2023). Intelligence-led Policing. Critical Publishing.

Kuckartz, U., & Radiker, S. (2023). Qualitative content analysis: Methods, practice and software.

Manual de doctrina de inteligencia Policial. (2022). Ministerio de Interior.

Montes, J. F. O. (2020). Estrategias Integradas de Ciberseguridad para el fortalecimiento de la Seguridad Nacional. *Revista de Ciencia e Investigación en Defensa*, *1*(4), 36-48.

Neale, B. (2021). The craft of qualitative longitudinal research: The craft of researching lives through time.

Ñaupas, H., Mejia, E., Trujillo, I., Romero, H., Medina, W., & Novoa, E. (2023). Metodología de la investigación total: Cuantitativa–Cualitativa y redacción de tesis 6a Edición. Ediciones de la U.

O'Malley, P. (2016). 'Policing the Risk Society'in the 21st Century. the 21st Century (February 8, 2016). Sydney Law School Research Paper, (16/11).

Piskors'ka, Y., Burda, A., & Roshko, I. (2020). Information security in Latin America. Науковий вісник Східноєвропейського національного університету імені Лесі Українки. Міжнародні відносини, (2 (406)).

Policía Nacional de Colombia. (2022). Biblioteca Escuela de Inteligencia y Contrainteligencia "Teniente Coronel Javier Antonio Uribe Uribe". Recuperado de https://www.policia.gov.co/escuelas/inteligencia/biblioteca

Rejas de la Peña, A. F., Huarcaya Hilares, W. A., Saavedra, J. A., & Veramendi Alhuay, G. (2025). Las aplicaciones de inteligencia artificial: herramientas esenciales para fortalecer la lucha contra la criminalidad. Arandu UTIC, 12(2), 670–691. https://doi.org/10.69639/arandu.v12i2.949

Rendón, A. D. Z., Talledo, Y. K. M., Mendoza, C. M. V., & Zambrano, A. R. R. (2024). Ciberataques en América Latina: desafíos de la era digital. Revista Compromiso Social, 89-104.

Rincón Arteaga, J. A., Castiblanco Hernández, S. A., Quijano Díaz, A., Urquijo Vanegas, J. D., & Pregonero León, Y. K. (2022). Ciberdelincuencia en Colombia: ¿qué tan eficiente ha sido la Ley de Delitos Informáticos? Revista criminalidad, 64(3), 95-116.

Rojas-Gutiérrez, W. J. (2022). La relevancia de la investigación cualitativa. Studium Veritatis, 20(26), 79-97.

Saavedra, B. (2023). Ciberseguridad en América Latina: Retos, Preocupaciones y Oportunidades. E. Ellis, y P. Vera, Desafíos y Amenazas a la Seguridad en América Latina, 1, 2-4.

Sarhan, M., Layeghy, S., Moustafa, N., & Portmann, M. (2023). Cyber threat intelligence sharing scheme based on federated learning for network intrusion detection. Journal of Network and Systems Management, 31(1), 3.

Sarkar, G., Singh, H., Kumar, S., & Shukla, S. K. (2023, August). Tactics, techniques and procedures of cybercrime: A methodology and tool for cybercrime investigation process. In Proceedings of the 18th International Conference on Availability, Reliability and Security (pp. 1-10).

Solar, C. (2023). Cybersecurity governance in Latin America: States, threats, and alliances. State University of New York Press.

Toapanta, S. M. T., Cobeña, J. D. L., & Gallegos, L. E. M. (2020). Analysis of cyberattacks in public organizations in Latin America. Adv. Sci. Technol. Eng. Syst, 5(2), 116-125.

Tounsi, W., & Rais, H. (2018). A survey on technical threat intelligence in the age of sophisticated cyber attacks. Computers & security, 72, 212-233.

Vera, M. D. B. (2023). El Ciberdelito, desafíos para la ley penal y civil. Marco jurídico nacional y comparado. Revista Jurídica, 7(1).

Villamizar Moreno, A. O., & Pedraza Uribe, L. F. (2023). Características metodológicas del análisis de información en la inteligencia policial de Colombia. Revista Logos Ciencia & Tecnología, 15(2), 87-106.

Wang, L., Lee, G., & Williams, I. (2019). The spatial and social patterning of property and violent crime in toronto neighbourhoods: A spatial-quantitative approach. ISPRS International Journal of Geo-Information, 8(1), 51.

Yang, S., Keller, F. B., & Zheng, L. (2016). Social network analysis: Methods and examples. Sage Publications.