Ciencia Latina Revista Científica Multidisciplinar, Ciudad de México, México.
ISSN 2707-2207 / ISSN 2707-2215 (en línea), mayo-junio 2026,
Volumen 10, Número 3.

https://doi.org/10.37811/cl_rcm.v10i3

CONTROL GUBERNAMENTAL DE LA CIBERINTELIGENCIA

GOVERNMENT CONTROL OF CYBERINTELLIGENCE

Aldo Fernando Rejas de la Peña
Escuela de Posgrado PNP, Peru

Heiner Olivares Muñoz
Escuela de Posgrado PNP, Peru

Br. Giancarlos Veramendi Alhuay
Escuela de Posgrado de la PNP, Peru

Br. Edwin Fernandez Huaman
Universidad Continental, Peru

DOI: https://doi.org/10.37811/cl_rcm.v10i3.24089

Control Gubernamental de la Ciberinteligencia

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

Heiner Olivares Muñoz
48142907@escpograpnp.com
https://orcid.org/0009-0005-5008-2504
Escuela de Posgrado PNP

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

Br. Edwin Fernandez Huaman
43590617@continental.edu.pe
https://orcid.org/0000-0004-2403-2610
Universidad Continental

RESUMEN

El presente trabajo explicar de qué manera el control gubernamental optimiza la ciberinteligencia, el estudio es de tipo básica o sustantiva, de enfoque cualitativo, el diseño de estudio es fenomenológico hermenéutico, La investigación se llevó a cabo en el contexto operativo del SIPOL, con la participación de analistas especializados en el desarrollo de recolección, análisis y difusión de información obtenida por Ciberinteligencia, la técnica e instrumento de recolección de datos para esta investigación se empleó la entrevista y la guía de entrevista semiestructurada. Se concluyó que el control gubernamental optimiza la ciberinteligencia al proporcionar un marco legal que regula y dirige las operaciones dentro de los límites éticos y eficientes. Los especialistas coinciden en que este control fortalece las capacidades de los operadores, permite una recolección oportuna de información y garantiza la adherencia a principios legales. No obstante, también surgen desafíos como la falta de normativas específicas y la burocracia que ralentiza la toma de decisiones. La mejora constante de las leyes y la capacitación del personal resultan cruciales para enfrentar las crecientes amenazas cibernéticas.

***Palabras claves*:** ciberinteligencia, control gubernamental, interno, judicial, legislativo

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

Government Control of Cyberintelligence

ABSTRACT

The present work explain how government control optimises cyberintelligence, the study is of basic or substantive type, qualitative approach, the study design is hermeneutic phenomenological, The research was conducted in the operational context of SIPOL, with the participation of analysts specialised in the development of collection, analysis and dissemination of information obtained by Cyberintelligence, the technique and instrument of data collection for this research was used the interview and the semi-structured interview guide. It was concluded that government control optimises cyberintelligence by providing a legal framework that regulates and directs operations within ethical and efficient limits. Specialists agree that this control strengthens the capacities of operators, enables timely collection of information and ensures adherence to legal principles. However, challenges also arise, such as the lack of specific regulations and the bureaucracy that slows down decision-making. Continuous improvement of laws and training of staff are crucial to address the growing cyber threats.

***Key words*:** cyberintelligence. governmental, internal, judicial, legislative control

Artículo recibido 25 marzo 2026
Aceptado para publicación: 25 abril 2026

INTRODUCCIÓN

El control gubernamental de la ciberinteligencia a nivel mundial ha evolucionado significativamente en respuesta a las crecientes amenazas cibernéticas. La vigilancia masiva, como se evidenció en el caso de Edward Snowden, ha suscitado un intenso debate sobre la necesidad de equilibrar la seguridad nacional con los derechos humanos (Chen, 2017). La implementación de marcos regulatorios más estrictos es esencial para prevenir abusos y garantizar que las actividades de inteligencia sean supervisadas adecuadamente (Nourkeyhani, 2018). Según Ho & Kallberg (2017), la creación de estándares internacionales puede ayudar a establecer límites claros sobre el uso de tecnologías de vigilancia.

Además, organismos como la ONU han instado a los países a adoptar políticas que prioricen la privacidad y la libertad de expresión en el ámbito digital (Chilano, 2024). Esto incluye la promoción de un marco ético que guíe las acciones gubernamentales en la ciberinteligencia, asegurando que las herramientas no se utilicen para reprimir a la sociedad civil (Zuboff, 2019). La colaboración internacional se vuelve crucial para enfrentar amenazas cibernéticas comunes y establecer protocolos que fortalezcan las capacidades nacionales sin comprometer los derechos fundamentales (OECD, 2020).

Por último, el desarrollo de alianzas entre gobiernos y el sector privado es fundamental para optimizar la ciberinteligencia. Estas colaboraciones permiten compartir información y recursos, lo que mejora la capacidad de respuesta ante incidentes cibernéticos (S2 Grupo, 2023). Un enfoque integral que incluya a múltiples actores puede contribuir a crear un entorno digital más seguro y resiliente frente a las amenazas emergentes.

En Latinoamérica, el control gubernamental sobre la ciberinteligencia enfrenta desafíos significativos debido a marcos regulatorios inconsistentes. Aunque muchos países han implementado leyes sobre ciberseguridad, su aplicación es variable y frecuentemente insuficiente para abordar el espionaje estatal (Aguilar Antonio, 2021). Por ejemplo, en México se han documentado casos del uso indebido de software de espionaje contra periodistas y activistas, lo que resalta la necesidad de mecanismos claros que regulen estas tecnologías (Cruz, 2021).

La falta de supervisión efectiva permite que las agencias gubernamentales utilicen herramientas tecnológicas sin justificación adecuada. Esto ha llevado a cuestionamientos sobre la efectividad del

control judicial previo requerido para operaciones especiales (Hiperderecho, 2019). La situación exige una reforma urgente en los marcos legales para asegurar que las actividades de inteligencia se alineen con los estándares internacionales en derechos humanos y protección de datos.

A pesar de los desafíos, están surgiendo iniciativas regionales prometedoras. La creación de redes para compartir información sobre ciberamenazas fomenta una mayor colaboración entre países, lo que es fundamental para enfrentar las amenazas transnacionales. Sin embargo, esta cooperación debe ir acompañada de un compromiso político sólido para establecer marcos legales que garanticen la transparencia, la rendición de cuentas y el respeto a los derechos humanos en las actividades de inteligencia.

En Perú, el control gubernamental sobre la ciberinteligencia está regido principalmente por el Decreto Legislativo N° 1141. Este marco legal establece procedimientos específicos para las actividades del Sistema Nacional de Inteligencia (SINA), pero ha sido criticado por su falta de claridad y por permitir un amplio rango de acciones sin suficientes salvaguardias (Hiperderecho, 2019). Las denuncias sobre abusos previos en el uso del espionaje han generado desconfianza hacia las instituciones encargadas.

La proliferación de herramientas tecnológicas ha facilitado que las agencias gubernamentales lleven a cabo una vigilancia masiva sin las debidas garantías legales. Esta práctica, evidenciada en numerosos casos recientes, ha socavado la privacidad de los ciudadanos y ha puesto en entredicho el control judicial sobre las operaciones especiales. La ausencia de límites claros en el uso de estas tecnologías ha generado un clima de desconfianza y ha exigido una revisión urgente del marco legal vigente.

Por último, es fundamental promover una cultura de transparencia en el gobierno peruano. La implementación efectiva del control gubernamental sobre la ciberinteligencia no solo requiere marcos legales sólidos, sino también un compromiso genuino con la protección de los derechos ciudadanos (Zuboff, 2019). Solo de esta manera se podrá establecer un sistema que optimice la seguridad nacional sin comprometer las libertades individuales. Fomentar esta cultura contribuirá a generar confianza en las instituciones y garantizar que las acciones de inteligencia se realicen dentro de un marco ético y responsable.

El presente trabajo de investigación evidencia cómo un control gubernamental eficaz puede potenciar significativamente las capacidades de la ciberinteligencia. Al establecer marcos legales claros y

mecanismos de supervisión rigurosos, se asegura que las actividades de inteligencia en el ciberespacio se realicen de manera legal, ética y eficiente. Esto permite a los organismos de inteligencia obtener, analizar y difundir información de manera oportuna, lo que contribuye a la toma de decisiones estratégicas y a la protección de los intereses nacionales. Un enfoque proactivo en la regulación y supervisión no solo mejora la efectividad operativa, sino que también fortalece la confianza pública en las instituciones encargadas de la seguridad nacional.

De lo antes mencionado se gesta el problema de investigación: ¿De qué manera el control gubernamental optimiza la ciberinteligencia?, de la misma forma se expresa los problemas específicos: ¿De qué manera el control legal optimiza la ciberinteligencia?, ¿De qué manera el control ético optimiza la ciberinteligencia? Y ¿De qué manera el control eficiente optimiza la ciberinteligencia?

El presente trabajo subraya la importancia del control gubernamental en la ciberinteligencia como pilar fundamental para la confianza pública. Un marco legal sólido y transparente, junto con mecanismos de supervisión independientes, asegura que las actividades de inteligencia se desarrollen legítima y responsablemente, fortaleciendo la relación Estado-ciudadanos y contribuyendo a la estabilidad nacional. En este mundo complejo, el control gubernamental emerge como activo estratégico para regular la ciberinteligencia, tendencia que exige adaptación tecnológica en la obtención, análisis y difusión informativa. La comunidad de inteligencia debe operar bajo estrictos parámetros de legalidad, ética y eficiencia, garantizando que las capacidades digitales sirvan al interés público mientras respetan derechos fundamentales y principios democráticos esenciales.

Este estudio ofrece una valiosa contribución a la comunidad de inteligencia al presentar un marco conceptual y metodológico que optimiza el control de las actividades de ciberinteligencia. Sus hallazgos son útiles para agentes y analistas a nivel mundial, proporcionando directrices claras para mejorar la recolección, análisis y difusión de información. Al enfatizar la legalidad, ética y eficiencia, este enfoque fortalece la efectividad operativa y promueve la confianza pública en las instituciones de seguridad. Además, establece bases sólidas para futuras investigaciones, identificando brechas en el conocimiento y proponiendo metodologías innovadoras que facilitan una comprensión más profunda de las dinámicas en la ciberinteligencia.

Ante ello se muestra el objetivo de la investigación*:* Explicar de qué manera el control gubernamental optimiza la ciberinteligencia de la misma forma se expresa los objetivos específicos: explicar de qué manera el control legal optimiza la ciberinteligencia, explicar de qué manera el control ético optimiza la ciberinteligencia y explicar de qué manera el control eficiente optimiza la ciberinteligencia.

Control gubernamental

El control gubernamental en el Sistema de Inteligencia Nacional (SINA) y la Dirección Nacional de Inteligencia (DINI), según establece la Ley N° 1141, comprende un proceso integral de supervisión, vigilancia y verificación de actividades estatales. La Contraloría General (2024) enfatiza que este control asegura la eficiencia, eficacia y transparencia en el uso de recursos públicos, mientras que Nourkeyhani (2018) destaca su rol fundamental en la prevención de abusos y en garantizar que las acciones de inteligencia se desarrollen dentro de marcos legales y éticos establecidos.

El control gubernamental se divide en interno y externo, proporcionando una evaluación completa de la gestión pública. Según Pinilla (2014), mientras el control interno se enfoca en medidas preventivas y correctivas institucionales, el control externo es ejecutado por entidades como la Contraloría General. Cabrera Ostertag (2016) sostiene que esta dualidad es crucial para mantener la integridad del sistema de inteligencia y garantizar decisiones basadas en información verificada. Neira Sánchez & Acosta Valdeleón (2011) enfatiza que un control efectivo es fundamental para la democracia, ya que promueve la rendición de cuentas y fortalece la legitimidad institucional mediante mecanismos transparentes de evaluación.

Control legal

El Sistema de Inteligencia Nacional (SINA) y la Dirección Nacional de Inteligencia (DINI) de Perú operan bajo el Decreto Legislativo N° 1141, que establece el marco regulatorio para actividades de inteligencia fundamentadas en legalidad, transparencia y derechos humanos. Como señala la DINI (2020), su principal objetivo es proteger la soberanía y promover el bienestar general, mientras que según Fernandez-Osorio et al. (2021), la DINI ejerce funciones de supervisión y control sobre los componentes del SINA para asegurar su eficiente funcionamiento.

El control legal del Sistema de Inteligencia Nacional incluye la supervisión del Congreso a través de la Comisión de Inteligencia, que según Gómez de la Torre & Medrano Carmona (2017) puede acceder a

información clasificada y evaluar el Plan Anual de Inteligencia. Hernández Sampieri et al. (2010) enfatizan que este control previene abusos y mantiene la confianza pública, mientras que de Oliveira & da Silva (2012) destaca la necesidad de autorización judicial para operaciones especiales según el Decreto Legislativo N° 1141. La UNODC (2015) señala que este enfoque equilibra la seguridad nacional con los derechos humanos, asegurando acciones de inteligencia efectivas y responsables.

Control ético

Según la Ley N° 1141, el SINA y la DINI deben realizar sus actividades de inteligencia bajo estrictos estándares de derechos humanos y principios legales claramente definidos. Como destaca Fernandez-Osorio et al. (2021), este marco normativo no solo representa una obligación jurídica sino también un imperativo moral, estableciendo controles éticos que previenen abusos y aseguran operaciones de inteligencia no discriminatorias orientadas al bien común y la protección de los derechos fundamentales. El control ético en actividades de inteligencia requiere una estricta rendición de cuentas supervisada por organismos independientes, especialmente el Congreso a través de su Comisión de Inteligencia, que fiscaliza al SINA. Montesinos (2014) enfatiza que esta supervisión legislativa es vital para la transparencia y prevención de abusos, mientras que Hernández Sampieri et al. (2010) señalan que la confianza pública depende de estos mecanismos democráticos. de Oliveira & da Silva (2012) destaca la importancia de proteger la información sensible, principio reforzado por el artículo 19 del D.L. N° 1141, mientras que UNODC (2015) subraya la privacidad como derecho fundamental en operaciones de inteligencia.

Control eficiente

La Ley N° 1141 reconoce el papel fundamental de las tecnologías de información y comunicación avanzadas para el control eficiente en el SINA y la DINI, estableciendo bases para la modernización del sistema. Fernandez-Osorio et al. (2021) enfatiza que este control debe ir más allá de la supervisión, optimizando recursos y procesos para garantizar una inteligencia oportuna y relevante mediante herramientas que mejoran la gestión informativa y la colaboración interinstitucional.

La coordinación efectiva en el SINA es crucial para la toma de decisiones informada, mediante la centralización de datos y protocolos claros que facilitan el análisis e identificación de amenazas. Montesinos (2014) destaca esta coordinación como fundamental, mientras que de Oliveira & da Silva

(2012) señala al PAI como marco orientador para la relevancia informativa. Yerrén (2022) enfatiza que la integración tecnológica mejora la capacidad de respuesta ante amenazas emergentes, y De La Cruz Reyes (2016)) subraya la importancia de la innovación para mantener la efectividad operativa, todo bajo la fiscalización transparente del Congreso.

Ciberinteligencia

La ciberinteligencia se define como el proceso de recopilación, análisis y aplicación de información sobre amenazas cibernéticas que pueden afectar a organizaciones y gobiernos. Este campo emergente combina la inteligencia tradicional con la tecnología de la información para anticipar, identificar y mitigar riesgos en el ciberespacio (Micronet, 2023). Según el Centro de Tecnologías Emergentes de la Universidad Carnegie Mellon, la ciberinteligencia permite a las entidades rastrear y predecir las actividades cibernéticas que podrían comprometer su seguridad (Santander Open Academy, 2024). En un entorno donde los ataques cibernéticos son cada vez más frecuentes y costosos, con un promedio de 270 incidentes por organización en 2021 (Foro Económico Mundial, 2021), la ciberinteligencia se convierte en una herramienta esencial para la defensa proactiva.

La ciberinteligencia abarca diversos tipos que permiten a las organizaciones enfrentar amenazas digitales emergentes. INESDI (2023) distingue entre la inteligencia estratégica, enfocada en analizar tendencias de ciberdelincuentes, y la táctica, que identifica amenazas inmediatas y actores específicos. Enthec (2023) describe la inteligencia operativa como enfoque en acciones preventivas concretas, mientras que Grupo Micronet (2023) resalta cómo esta clasificación mejora la protección de activos digitales. Sánchez Negrín (2024) enfatiza su rol en la identificación de vulnerabilidades y medidas preventivas, y INESDI (2023) destaca su contribución al cumplimiento normativo y protección de datos sensibles.

METODOLOGÍA

La investigación básica es una inversión fundamental para el avance científico y tecnológico a largo plazo, posicionándose como el motor del conocimiento, según Zuñiga et al. (2023), y como un catalizador clave para la innovación y la creatividad, de acuerdo con Fuster Guillen (2019). Su contribución va más allá, siendo esencial en la formación de investigadores altamente capacitados, a quienes les brinda el espacio para explorar fenómenos naturales sin presiones inmediatas.

Este enfoque metódico y profundo es precisamente el que sienta las bases para futuros descubrimientos significativos que terminan beneficiando a toda la sociedad.

El método inductivo construye teorías y generalizaciones partiendo de observaciones específicas. Hernández Samperio & Mendoza (2018) destacan su capacidad para formular conclusiones generales basadas en patrones emergentes, mientras que Sánchez (2018) resalta su utilidad en estudios exploratorios con teoría insuficiente. Este método fomenta una comprensión profunda mediante la adaptación flexible a nuevos datos, permitiendo generar teorías ajustadas a las realidades observadas.

El enfoque cualitativo es fundamental para construir teorías a partir de la exploración de experiencias vividas. Hernández Samperio & Mendoza (2018) destacan su capacidad para generar nuevos conceptos mediante la comprensión profunda de fenómenos sociales, mientras que Sánchez (2018) enfatiza su utilidad en investigaciones exploratorias y en el estudio de fenómenos en su contexto natural. Valdez (2018) resaltan su flexibilidad para adaptarse a las particularidades de cada situación estudiada.

El diseño de investigación fenomenológico es una metodología que se enfoca en comprender la esencia de las experiencias vividas desde la perspectiva de los propios individuos. Según Hernández Samperio & Mendoza (2018), este enfoque integra la descripción de dichas vivencias con su interpretación dentro de un contexto histórico y cultural. De este modo, logra trascender lo superficial para adentrarse en los significados profundos que los sujetos atribuyen a sus realidades, tal como destaca Sánchez (2018). En definitiva, el objetivo es capturar la experiencia subjetiva para ofrecer una comprensión rica y matizada de cómo las personas construyen sentido a partir de sus realidades cotidianas, según señalan Fuster Guillen (2019).

En el marco de una investigación, los participantes y los especialistas desempeñan roles esenciales y complementarios que enriquecen la calidad del estudio. Por un lado, los participantes aportan perspectivas únicas y auténticas, fundamentadas en sus experiencias directas con el fenómeno estudiado (Hernández Samperio & Mendoza, 2018). A su vez, los especialistas complementan esta visión aplicando un análisis crítico y riguroso, basado en su conocimiento experto y teórico (Sánchez, 2018). Según Valdez (2018), es precisamente esta sinergia entre la experiencia vivida y el análisis académico lo que permite construir una comprensión mucho más completa e integral del objeto de estudio.

La presente investigación se realizó con cuatro participantes dos agentes y dos analistas en inteligencia policial, quienes laboran en la Dirección de Inteligencia, seleccionados por su vasta experiencia y capacitación en la comunidad de inteligencia policial. El criterio de inclusión requería una probada especialización en control gubernamental y un profundo conocimiento de la cultura organizacional. Por ello, se excluyó a personal que no cumplía con este perfil altamente calificado. La contribución de estos participantes fue crucial, pues su habilidad para evaluar críticamente la información y detectar sesgos resultó esencial para formular conclusiones sólidas y confiables. Su participación demuestra que la experiencia especializada es un factor determinante para el éxito de las operaciones de inteligencia en contextos de alta complejidad informativa.

Tabla 1 Participantes o especialistas

Código	Característica	Experiencia	Funciones
EE1	Oficial superior	25 años	Agente y analista.
EE2	Oficial subalterno	5 años	Agente y analista.
EE3	Suboficial técnico	19 años	Agente y analista.
EE4	Suboficial técnico	18 años	Agente jefe de grupo

Nota: Elaboración propia (2024)

La entrevista es una técnica cualitativa esencial para profundizar en las experiencias de los participantes, permitiendo obtener datos ricos a través de la interacción directa (Hernández Sampieri & Mendoza, 2018). Su flexibilidad, ya sea estructurada o no, se adapta a diversos contextos (Sánchez, 2018), y captura matices que otras técnicas no logran, ofreciendo una visión holística del fenómeno (Fuster Guillen, 2019). A diferencia de los cuestionarios, que son más rígidos, la guía de entrevista no estructurada facilita una exploración abierta, siendo crucial un buen diseño para asegurar la calidad de los datos.

El análisis de datos cualitativos se enfoca en descifrar patrones y significados profundos, priorizando la complejidad de las experiencias humanas mediante un proceso iterativo de codificación y categorización (Hernández Sampieri & Mendoza, 2018; Sánchez, 2018). Para esta investigación, dicho enfoque se aplicará utilizando el *software ATLAS.ti* para examinar las entrevistas realizadas. A través de esta herramienta, se identificarán sistemáticamente las congruencias en las narrativas de los

participantes. Posteriormente, se realizará una contrastación de sus testimonios para hallar tanto coincidencias como discrepancias clave en relación con los objetivos del estudio, lo que permitirá construir una interpretación robusta y con mayor profundidad para sustentar los resultados de la investigación.

Resultado de investigación

Se fundamenta en las entrevistas de cuatro miembros del sistema de inteligencia policial especializados en ciberinteligencia: dos agentes y dos analistas. A través de sus testimonios, se exploró la práctica de la inteligencia en el ciberespacio, enmarcada por un control gubernamental que exige pertinencia legal, ética y eficiencia. Un eje central del discurso fue la imperativa necesidad de conducir sus operaciones con un irrestricto respeto a los derechos humanos, reflejando su identidad como profesionales probos y su profundo compromiso con una conducta íntegra en el ejercicio de sus delicadas funciones. Para el presente análisis se contó con el *Software ATLAS.ti. mostrando a continuación las figuras obtenidas.*

Figura 1 Nube de palabras

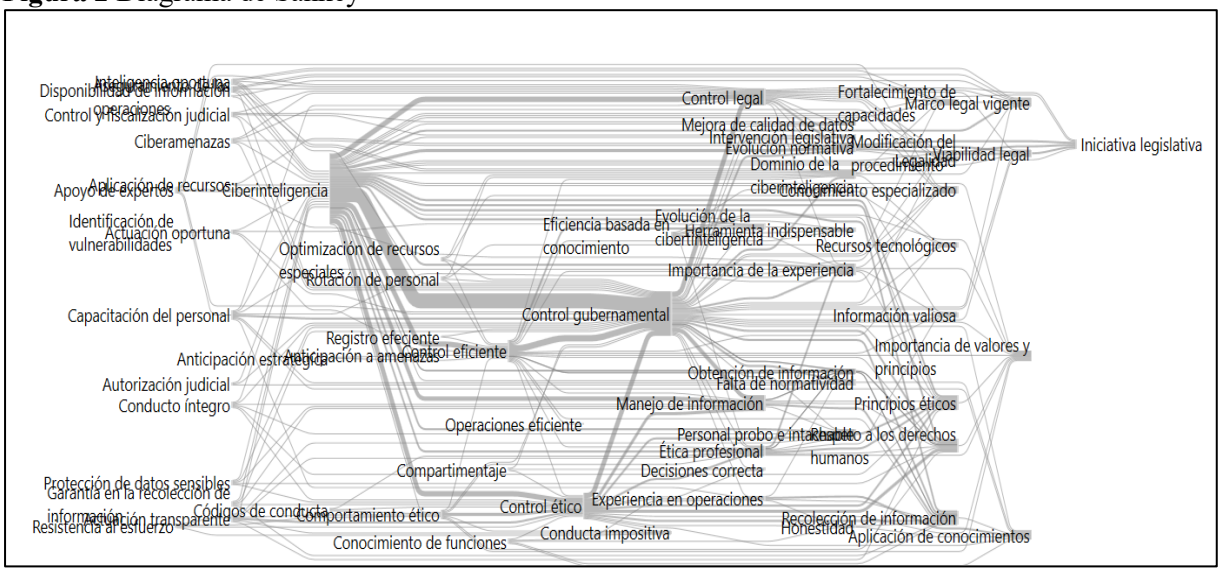
Nota: datos obtenidos del análisis de las entrevistas en el Software ATLAS.ti.

La nube de palabras revela que el control gubernamental optimiza la ciberinteligencia al establecer un marco robusto de legalidad y legitimidad. La prominencia de términos como *"información", "principios", "procedimientos", "normas" y "ley"* sugiere que el control no se concibe como una

limitación, sino como la estructura indispensable para la acción. Este andamiaje ético y legal, que incluye la *"transparencia"* y la protección de *"información personal"*, es el mecanismo principal para garantizar que las *"operaciones"* se realicen de manera *"correcta"* y segura, transformando la recolección de datos en un proceso ordenado y fiable.

El análisis evidencia que esta optimización se materializa a través del *"personal"* especializado. El control gubernamental dota a los *"agentes"* y al *"equipo policial"* de *"herramientas"* y directrices claras para actuar frente a amenazas. La interacción de conceptos como *"seguridad", "decisiones" y "análisis"* indica que un control efectivo mejora la calidad del producto de inteligencia. Al alinear las *"operaciones"* con los marcos *"legislativos"* y los *"principios éticos"*, el control gubernamental no solo optimiza la eficiencia, sino que fortalece la confianza y la efectividad de las acciones de ciberinteligencia en el contexto peruano.

Figura 2 Diagrama de Sankey



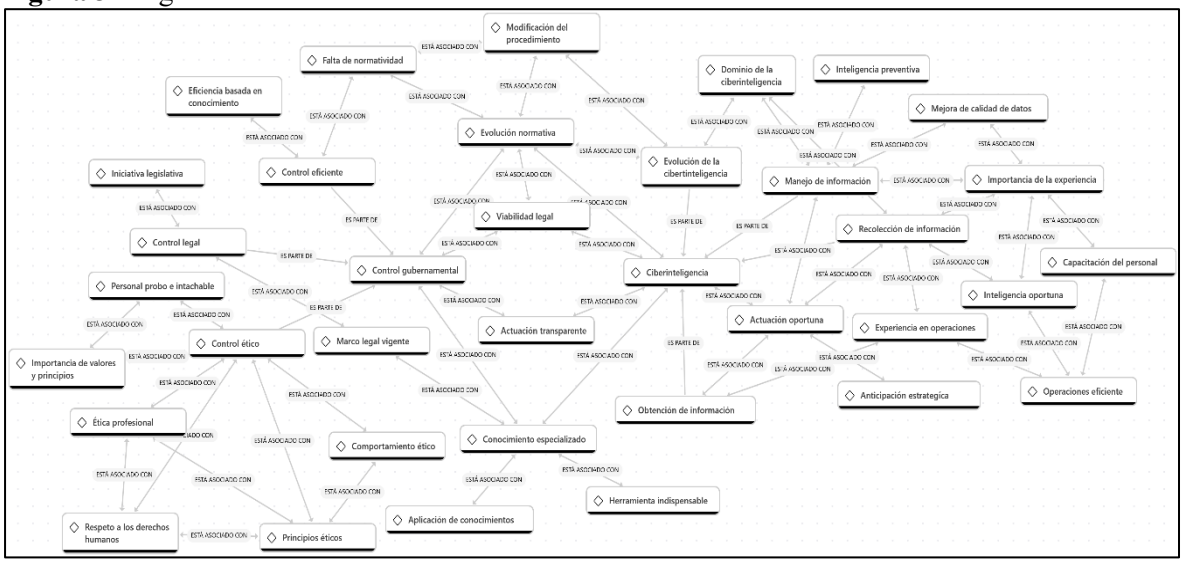
Nota: datos obtenidos del análisis de las entrevistas en el Software ATLAS.ti

El análisis del diagrama de Sankey revela que el "Control gubernamental" se erige como el nodo articulador central en el discurso de los agentes y analistas, confirmando su papel preponderante en la optimización de la ciberinteligencia. Este concepto no es un fin en sí mismo, sino un mediador que canaliza problemáticas operativas como las "Ciberamenazas" y la necesidad de "Optimización de recursos" hacia soluciones estructurales. La fuerte co-ocurrencia entre estas categorías de entrada y el "Control gubernamental" sugiere que, para los expertos, la supervisión estatal es la respuesta directa a

los desafíos tácticos y estratégicos del dominio cibernético, actuando como el principal catalizador para transformar las necesidades operativas en acciones de alto nivel.

La optimización se materializa, según el flujo del diagrama, en una dimensión marcadamente normativa y legal. El "Control gubernamental" fluye de manera contundente hacia el "Fortalecimiento de Marco legal vigente" y, en última instancia, hacia la "Iniciativa legislativa". Esto indica que los entrevistados no conciben una ciberinteligencia optimizada sin un andamiaje jurídico robusto y actualizado que la respalde. De forma paralela, el control se vincula con la generación de "Información valiosa" y el "Control ético", demostrando que la optimización no solo se persigue en términos de eficiencia, sino también de legitimidad, calidad de la inteligencia y respeto a los principios fundamentales.

Figura 3 Diagrama de Redes



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

El diagrama de redes semánticas sitúa al "Control gubernamental" como un concepto de alta centralidad, directamente conectado con la "Ciberinteligencia". A diferencia de un flujo lineal, esta red revela que el control se construye sobre pilares fundamentales: el "Control legal" y el "Control eficiente", los cuales a su vez se asocian con un "Marco legal vigente" y una "Iniciativa legislativa". Esto demuestra que, desde la perspectiva de los expertos, el control no es una acción abstracta, sino una estructura multifacética que integra la supervisión jurídica, la eficiencia operativa y la ética, representada por su conexión con el "Control ético", para dar forma a un ecosistema de inteligencia robusto.

La optimización de la “Ciberinteligencia” se produce a través de la influencia directa de este control estructurado. El “Control gubernamental” se asocia fuertemente con la “Viabilidad legal”, un nodo puente que a su vez se conecta con la “Evolución de la ciberinteligencia” y la “Modificación del procedimiento”. Esto sugiere que el control gubernamental optimiza al proporcionar la seguridad y el respaldo jurídico necesarios para que las prácticas de ciberinteligencia evolucionen, se adapten y mejoren la calidad de sus datos. En esencia, el control no la restringe, sino que la habilita, creando un entorno seguro para su perfeccionamiento y operación eficaz.

Tras realizar el análisis mediante el *software ATLAS.ti*, se efectuó la contrastación de las entrevistas identificando dos párrafos coincidencias y dos párrafos de discrepancias en concordancia con los objetivos de la investigación:

Objetivo de investigación: **Explicar de qué manera el control gubernamental optimiza la ciberinteligencia.**

Los entrevistados coinciden en que el control gubernamental, a través de la normativa legal, juega un papel crucial en la optimización de la ciberinteligencia, brindando un marco regulatorio que asegura el cumplimiento ético y eficiente en las operaciones. Especialistas como ET2 y ET3 mencionan que las leyes fortalecen las capacidades de los operadores, proporcionando inteligencia oportuna para enfrentar amenazas a la seguridad. Además, todos coinciden en que las normativas ayudan a actuar de manera rápida y adecuada ante las vulnerabilidades, garantizando así que las operaciones se mantengan dentro de los márgenes éticos y legales establecidos.

También, los entrevistados resaltan la importancia de la supervisión judicial y legislativa, la cual mejora la calidad de los datos y análisis al asegurar que los procedimientos se adhieran a estándares legales. Según ET1 y ET4, el control judicial proporciona un nivel de fiscalización que refuerza la legitimidad y precisión de las operaciones de ciberinteligencia, mientras que ET2 añade que los ajustes normativos constantes son necesarios para mantenerse al día con las amenazas cibernéticas emergentes.

Por otro lado, algunos especialistas destacan discrepancias en la implementación práctica de estas normativas. ET1 señala que en Perú no existe una normativa específica sobre ciberinteligencia, lo que limita las operaciones a regulaciones más generales como la ley de delitos informáticos, afectando la agilidad operativa debido a la burocracia y la necesidad de autorizaciones judiciales. ET3 coincide al

mencionar la falta de preparación adecuada del personal, lo que obliga a recurrir a expertos externos en algunas situaciones, lo que puede ralentizar la respuesta ante amenazas.

Adicionalmente, ET2 y ET3 identifican desafíos en la capacitación del personal y en la correcta aplicación de los procedimientos legales, lo cual puede generar una dependencia en la experiencia individual más que en un marco estructurado y estandarizado. Esta situación puede reducir la eficiencia operativa y afectar la capacidad de las instituciones para prevenir y reaccionar rápidamente ante ataques cibernéticos, mostrando una disparidad entre la teoría normativa y la práctica diaria.

Del objetivo específico 1: Explicar de qué manera el control legal optimiza la ciberinteligencia.

Los entrevistados perciben que las normativas legales vigentes en el Perú tienen un impacto considerable en las operaciones de ciberinteligencia, aunque no existe una ley específica sobre el tema. Según el especialista ET1, las normativas actuales, como la ley de delitos informáticos, permiten operar dentro de un marco regulatorio, pero requieren autorización judicial para actividades clave, como la videovigilancia y la interceptación de comunicaciones. Esto establece un marco legal básico, que, si bien no es específico para ciberinteligencia, da una estructura mínima para el accionar dentro de los límites legales.

Asimismo, ET2 destaca que las normas legales son esenciales para fortalecer las capacidades operativas de los agentes, permitiéndoles actuar con inteligencia oportuna ante amenazas a la seguridad del Estado. ET3 también subraya la importancia de las normativas para enfrentar amenazas de manera eficiente, argumentando que estas leyes permiten actuar de manera proactiva. Además, ET4 menciona que la evolución de las normativas nacionales e internacionales con el tiempo contribuye a mitigar las ciberamenazas, lo que refuerza la percepción de que la regulación es clave para una ciberinteligencia efectiva y legalmente respaldada.

A pesar del consenso general sobre la relevancia de un marco normativo, surgen algunas discrepancias entre los entrevistados respecto a su implementación. ET1 menciona un obstáculo importante relacionado con la burocracia, señalando que las autorizaciones judiciales necesarias para operaciones clave ralentizan la ejecución de estas. Esta percepción contrasta con la visión de ET4, quien afirma que las normativas legales permiten una ejecución operativa ajustada a las leyes, sin mencionar problemas

de burocracia o demoras. Además, ET1 resalta la falta de apoyo de las empresas privadas, lo que no es mencionado por los otros especialistas.

Otro punto de discrepancia es la capacitación y preparación del personal. Mientras ET2 aboga por una mayor formación teórica para asegurar que las operaciones no vulneren derechos, ET3 admite que en muchos casos no se cuenta con la preparación suficiente, dependiendo de expertos externos para llevar a cabo procedimientos de manera adecuada. Esta diferencia refleja un desafío interno en el fortalecimiento del capital humano para optimizar el uso del marco legal en operaciones de ciberinteligencia.

Objetivo Específico 2: Explicar de qué manera el control ético optimiza la ciberinteligencia.

Los entrevistados coinciden en la importancia de los principios éticos como un pilar fundamental en las operaciones de ciberinteligencia, especialmente en el manejo de información sensible. Según el especialista ET1, es esencial tratar la información con responsabilidad y respeto a los derechos humanos, lo que establece una base ética firme en la recolección de datos. ET3 y ET4 refuerzan esta visión, afirmando que el personal que maneja dicha información debe actuar con probidad y garantizar que sus decisiones sean conformes a las atribuciones legales. ET4 también añade que se debe designar personal intachable, lo que implica que la ética no solo se refleja en las acciones, sino en la selección de los operadores.

Asimismo, todos los especialistas coinciden en que los dilemas éticos son inevitables en operaciones de ciberinteligencia. ET1 menciona que la información que no tiene relevancia con la investigación debe ser desechada, mientras que ET3 y ET4 hablan de la necesidad de mantener los principios de transparencia y honestidad ante situaciones de corrupción o soborno. En conjunto, los entrevistados subrayan que los principios éticos, como la transparencia y la integridad, son esenciales para garantizar que la ciberinteligencia se ejecute dentro de los parámetros legales y morales adecuados.

A pesar de este consenso, hay diferencias en cómo se percibe la aplicación práctica de estos principios éticos. ET2, por ejemplo, plantea que no todas las personas dentro de la organización reaccionan de la misma manera ante los dilemas éticos, mencionando que algunos son más débiles o se ven tentados a actuar en contra de los principios éticos. Esto contrasta con la visión de ET4, quien cree que los códigos

de conducta éticos son claros y necesarios para establecer limitaciones y garantizar el respeto dentro de la organización, sugiriendo que las normas pueden prevenir el mal comportamiento.

Otra discrepancia surge en la percepción sobre cómo gestionar los dilemas éticos. ET3 pone el énfasis en el ofrecimiento de dádivas por parte de terceros y la necesidad de actuar con transparencia, mientras que ET4 destaca dilemas relacionados con actos de corrupción y violaciones de derechos humanos, como la tortura. Esta diferencia refleja una variabilidad en las situaciones éticas a las que se enfrentan los operadores y en la gravedad de estas, lo que sugiere que los desafíos éticos en ciberinteligencia pueden tener diferentes niveles de complejidad según el contexto.

Objetivo Específico 3: Explicar de qué manera el control eficiente optimiza la ciberinteligencia.

Los entrevistados coinciden en que la eficiencia en el uso de los recursos tecnológicos y humanos es crucial para optimizar las operaciones de ciberinteligencia. ET1 subraya la importancia de evitar la rotación del personal especializado y de contar con equipos informáticos de alta gama destinados específicamente a las divisiones de ciberinteligencia. Este énfasis en la estabilidad del personal especializado también es compartido por ET4, quien destaca la necesidad de una capacitación constante para mantener al personal actualizado ante la evolución de las amenazas cibernéticas. ET3 complementa esta visión al mencionar que la implementación tecnológica avanzada es esencial para garantizar la eficiencia en las operaciones.

Además, los especialistas coinciden en que la eficiencia en las operaciones de ciberinteligencia tiene un impacto directo en la toma de decisiones estratégicas. ET1 señala que una operación eficiente permite a las fuerzas de seguridad adelantarse a las acciones de los actores hostiles, mientras que ET2 y ET3 recalcan que el conocimiento, la experiencia y el trabajo en equipo son factores clave para obtener información valiosa y procesarla de manera efectiva. Esta información es crítica para prevenir amenazas y tomar decisiones acertadas en el contexto de la ciberseguridad.

Sin embargo, hay diferencias en las percepciones sobre qué aspectos son prioritarios para garantizar la eficiencia. Mientras que ET2 considera que la organización y los registros son esenciales para optimizar las operaciones, ET1 y ET3 ponen mayor énfasis en la tecnología avanzada como el hardware y software de alta gama. ET3, además, sugiere que la eficiencia depende no solo de los recursos logísticos sino también del trabajo en equipo entre personal capacitado, mientras que ET2 prioriza la correcta

organización y el interés general por encima de todo, lo que sugiere una variación en las prioridades organizativas.

Otra discrepancia se refiere a la importancia atribuida al control de seguridad y la capacitación continua. ET4 resalta la necesidad de controlar la seguridad y evitar pérdidas de información mediante el uso de claves y otros controles, mientras que ET1 se centra más en el factor humano, señalando que un personal altamente capacitado y especializado es el elemento más importante para asegurar la eficiencia. Aunque ambos especialistas valoran la formación del personal, ET4 da más peso a las medidas de control y protección de la información, mientras que ET1 prioriza la especialización continua del personal sobre otros factores.

CONCLUSIONES

El control gubernamental optimiza la ciberinteligencia al proporcionar un marco legal que regula y dirige las operaciones dentro de los límites éticos y eficientes. Los especialistas coinciden en que este control fortalece las capacidades de los operadores, permite una recolección oportuna de información y garantiza la adherencia a principios legales. No obstante, también surgen desafíos como la falta de normativas específicas y la burocracia que ralentiza la toma de decisiones. La mejora constante de las leyes y la capacitación del personal resultan cruciales para enfrentar las crecientes amenazas cibernéticas.

El control legal optimiza la ciberinteligencia al proporcionar un marco normativo que permite a los operadores actuar de manera legal y eficiente frente a amenazas cibernéticas. Aunque no existe una legislación específica en el Perú, las normativas actuales, como la ley de delitos informáticos, ofrecen una estructura básica que regula operaciones clave. No obstante, surgen desafíos como la burocracia y la falta de capacitación adecuada del personal, lo que ralentiza las operaciones. En conjunto, las normativas legales fortalecen la capacidad de respuesta, pero requieren ajustes para mejorar su aplicación práctica y operativa.

El control ético optimiza la ciberinteligencia al asegurar que las operaciones se realicen dentro de un marco de integridad y respeto por los derechos humanos. Los entrevistados coinciden en que la ética es fundamental para manejar información sensible de manera responsable, garantizando transparencia y honestidad en cada decisión. Además, la probidad del personal y la correcta gestión de dilemas éticos,

como el rechazo a la corrupción, son clave para mantener la legitimidad de las operaciones. Sin embargo, surgen desafíos relacionados con la uniformidad en la aplicación de estos principios dentro de las organizaciones.

El control eficiente optimiza la ciberinteligencia al maximizar el uso de recursos tecnológicos y humanos, mejorando la respuesta ante amenazas cibernéticas. Los entrevistados coinciden en que contar con personal especializado y tecnología avanzada es esencial para la eficiencia operativa. Además, la toma de decisiones estratégicas se ve reforzada cuando las operaciones son fluidas y organizadas, permitiendo anticiparse a posibles ataques. Sin embargo, surgen diferencias en las prioridades, con algunos especialistas enfocándose en la organización y registros, mientras que otros resaltan la capacitación constante y el control de la seguridad.

REFERENCIAS BIBLIOGRAFICAS

Academia Abierta de Santander. (2022). Ciberinteligencia. Blog Academia Abierta de Santander.

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.

Cabrera Ostertag, R. J. (2016). Control ético y profesional de las profesiones liberales: diagnóstico a la norma jurídica vigente: un análisis dogmático a la normativa legal vigente, doctrina, jurisprudencia y sus consecuencias.

Contraloría General. (2024). Normas Generales de Control Gubernamental. Recuperado de https://www.gob.pe/institucion/contraloria/informes-publicaciones/2465590-normas-de-control-de-la-contraloria

Chen, K. (2017). No place to hide: Edward Snowden, the NSA, and the US surveillance state.

Chilano, B. M. (2024). Intimidad en la era digital: análisis jurídico y enfoque juvenil sobre percepciones y prácticas. Derecom, (35), 3.

de Oliveira Junior, A., & da Silva, E. B. (2012). Cooperación internacional e inteligencia en el combate de la criminalidad transnacional: el Caso Brasileño. *Policía y seguridad pública*, 1(2), 131-152.

De La Cruz Reyes, C. M. (2016). Propuesta de implementación de control interno para mejorar la unidad de logística de la municipalidad distrital de condebamba año-2017.

DINI. (2020). Informe sobre Cooperación Internacional. Dirección Nacional de Inteligencia.

Fernández-Osorio, A. E., Payá-Santos, C., & Mirón, M. (2021). Perspectiva histórica y doctrinas estratégicas en inteligencia. *Revista Científica General José María Córdova*, 19(36), 837-849.

Foro Económico Mundial. (2021). Perspectivas mundiales sobre ciberseguridad 2021.

Fuster Guillen, D. E. (2019). Investigación cualitativa: Método fenomenológico hermenéutico. Propósitos y representaciones, 7(1), 201-229.

Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, M. (2010). Metodología de la Investigación. McGraw-Hill.

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

Hiperderecho. (2019). Sistema nacional de inteligencia y privacidad. Recuperado de https://hiperderecho.org/2019/06/sistema-nacional-de-inteligencia-y-privacidad/

Ho, M., & Kallberg, J. (2017). Black Code: Surveillance, Privacy, and the Dark Side of the Internet.

INESDI. (2023). ¿Qué es la Ciberinteligencia?, ¿Por qué es Necesaria? BlogINESDI https://www.inesdi.com/blog/ciberinteligencia-que-es/#:~:text=La%20ciberinteligencia%20es%20la%20recopilaci%C3%B3n,el%20uso%20de%20la%20red.

Grupo Micronet (2023). ¿Qué es la Ciberinteligencia? Blog Micronet. https://blog.grupomicronet.com/que-es-la-ciberinteligencia#:~:text=La%20ciberinteligencia%20es%20el%20proceso,vigilancia%20en%20el%20%C3%A1mbito%20digital.

Gómez de la Torre, A., & Medrano Carmona, A. (2017). Orígenes en el proceso de inteligencia en el Perú. URVIO *Revista Latinoamericana de Estudios de Seguridad*, (21), 104-120.

Neira Sánchez, F. O., & Acosta Valdeleón, W. (2011). Ética en las profesiones: tendencias y desafíos. Universidad de la Salle.

Nourkeyhani, B. (2018). Surveillance in Digital Technology as a Threat to Democracy.

OECD. (2020). Digital Transformation for Building Back Better. Recuperado de https://www.oecd-ilibrary.org/docserver/4c1df5c7-

es.pdf?accname=guest&checksum=9BA20251C56039B14773F5687A1F705C&expires=1726484513&id=id

ONUDD. (2015) Contra la Delincuencia Organizada Transnacional.

Pinilla, F. S. (2014). El concepto de "control" en el régimen colombiano de integraciones empresariales y sus implicaciones frente a la adquisición de participaciones minoritarias. *Revista de derecho de la competencia CEDEC*, 10(10), 457-497.

S2 Grupo. (2023). Entrevista a Enrique Fenollosa. Recuperado de https://www.segurilatam.com/ciberilatam/ciberseguridad-ciberilatam/s2-grupo-incidentes-recientes-evidencian-como-un-ciberataque-puede-paralizar-un-pais_20240410.html

Sánchez, M. (2018). Fundamentos del método inductivo. Investigación y Ciencia.

Sánchez Negrin, M. F. (2024). Normativas y Marco Legal en Ciberseguridad, Evolución de Amenazas Cibernéticas y Aspectos Éticos de la Ciberseguridad.

Santander Open Academy. (2024). Ciberinteligencia: Qué es y cómo funciona. https://www.santanderopenacademy.com/es/blog/ciberinteligencia.html

Valdés, J. (2018). Investigación Cualitativa–Claves teóricas y prácticas. https://abacoenred.org/wp-content/uploads/2016/01/Investigacion-cualitativa-claves-te%C3%B3ricas-y-pr%C3%A1cticas.pdf

Yerrén, R. H. (2022). El sistema de control interno y la gestión pública: Una revisión sistemática. *Ciencia Latina Revista Científica Multidisciplinar*, 6(2), 2316-2335.

Zuboff, S. (2019). The age of surveillance capitalism: The fight for a human future at the new frontier of power, edn. PublicAffairs, New York.

Zúñiga, P. I. V., Cedeño, R. J. C., & Palacios, I. A. M. (2023). Metodología de la investigación científica: guía práctica. *Ciencia Latina Revista Científica Multidisciplinar*, 7(4), 9723-9762.