
# Ciberdefensa y Ciberseguridad para la lucha Contra el Narcotráfico y Amenazas Trasnacionales.

Mayor (EJC) Yerson Enrique Suarez Rojas

Artículo para optar al título profesional:

Magister en Tecnología e Innovación en Defensa

Escuela Superior de Guerra "General Rafael Reyes Prieto"
Bogotá D.C., Colombia
2025

**Escuela Superior de Guerra "General Rafael Reyes Prieto"**
Bogotá D.C., Colombia

| DATOS GENERALES | | |
|---|---|---|
| **Nombre del estudiante** | **:** | Mayor (EJC) Yerson Enrique Suarez Rojas |
| **Identificación** | **:** | 1.026.255.997 |
| **Programa académico** | **:** | Maestría en Ciberseguridad |
| **Tutor metodológico** | **:** | Dr. Jairo Andrés Becerra Cuervo |
| **Tutor temático** | **:** | |
| **Fecha de entrega** | **:** | 20 de junio de 2025 |
| **Extensión** | **:** | |

**DECLARACIÓN DE ORIGINALIDAD Y CESIÓN DE DERECHOS**

El autor declara que esta monografía fue escrita de acuerdo con la normatividad de la Escuela Superior de Guerra "General Rafael Reyes Prieto" (ESDEG) y no existe ningún potencial conflicto de interés relacionado con este. Las posturas y aseveraciones presentadas son resultado de un ejercicio académico e investigativo que no representan la posición oficial ni institucional de la ESDEG, las Fuerzas Militares de Colombia o el Ministerio de Defensa Nacional.

Esta monografía es enteramente mi propio trabajo y no ha sido presentada para la obtención de un título en esta u otra Institución de Educación Superior. Se han referenciado todos los trabajos y puntos de vista de otros autores, así como los datos de otras fuentes utilizadas. No se emplearon herramientas de generación de contenido por Inteligencia Artificial para su elaboración.

El autor acepta ceder los derechos de publicación en favor de la ESDEG y su Sello Editorial de acuerdo con los términos de la licencia Creative Commons: Reconocimiento-NoComercial-SinObrasDerivadas.

**AUTORIZACIÓN DE PUBLICACIÓN**

El autor autoriza que esta monografía sea publicada por el Sello Editorial ESDEG en su repositorio institucional y esté disponible bajo una modalidad de acceso abierto.

**Escuela Superior de Guerra "General Rafael Reyes Prieto"**
Bogotá D.C., Colombia

# Ciberdefensa y Ciberseguridad para la lucha Contra el Narcotráfico y Amenazas Trasnacionales.

## Cyberdefense and Cybersecurity in the Fight Against Drug Trafficking and Transnational Threats.

**Yerson Enrique Suarez Rojas** [1]
Escuela Superior de Guerra "General Rafael Reyes Prieto"

**Resumen:**
Este análisis examina cómo el ciberespacio se ha convertido en un escenario clave para el accionar de redes criminales de alcance internacional, centrando la atención en las amenazas informáticas vinculadas al tráfico de drogas. Se sostiene que las estructuras delictivas han incorporado avances tecnológicos para diversificar y sofisticar sus métodos de operación, utilizando recursos como activos digitales, redes virtuales privadas, aplicaciones de mensajería encriptada, software malicioso y técnicas de alteración digital. Dichas herramientas no solo facilitan la evasión de los sistemas de control estatales, sino que fortalecen la capacidad de operar con anonimato, de forma distribuida y a escala transnacional. En este marco, el propósito del artículo es detectar nuevas amenazas en el entorno digital relacionadas con el narcotráfico y delitos conexos, construir un modelo de análisis riguroso y aplicar dicho esquema con el fin de generar propuestas de actuación para los Estados y organismos multilaterales. En cuanto al enfoque metodológico, se adopta una perspectiva cualitativa de corte exploratorio, sustentada en el análisis crítico de fuentes documentales. El análisis se apoya en las teorías de Johan Galtung y Elsa Blair Trujillo, las cuales permiten comprender que la violencia cibernética va más allá de los daños tecnológicos, expresando dimensiones más amplias como desigualdad estructural, dominación simbólica y conflictos sociales no resueltos. Desde esta mirada, se plantea que las amenazas digitales deben interpretarse tanto en su funcionamiento técnico como en sus raíces sociopolíticas profundas. Como resultado, se argumenta que el ecosistema digital ha transformado profundamente la naturaleza de la criminalidad moderna, exigiendo una renovación normativa, ética y estratégica en materia de ciberdefensa. Se subraya la urgencia de establecer mecanismos de cooperación internacional basados en inteligencia colaborativa, vigilancia avanzada y enfoques integrales que incorporen dimensiones sociales, económicas y políticas. Así, la ciberseguridad se redefine como una estrategia sistémica que busca salvaguardar la democracia, la soberanía tecnológica y los derechos fundamentales ante entornos complejos y en constante mutación.

[1] Mayor del Ejército Nacional de Colombia. Candidato a magíster en Ciberseguridad y Ciberdefensa, Escuela Superior de Guerra "General Rafael Reyes Prieto", Colombia. Profesional en Ciencias Militares, Escuela Militar de Cadetes "General José María Córdova", Colombia. https://orcid.org/0000-0003-2004-7466 - Contacto: yerson.suarez@esdeg.edu.co.

**Palabras clave:** Ciberespacio; Ciberdefensa; Cooperación internacional Narcotráfico; Violencia

**Abstract:**

This study explores how cyberspace has become a critical arena for the operations of internationally connected criminal networks, with a specific focus on cyber threats linked to drug trafficking. It argues that criminal structures have incorporated technological advancements to diversify and enhance their operational methods, employing tools such as digital assets, virtual private networks, encrypted messaging applications, malicious software, and digital manipulation techniques. These technologies not only facilitate the evasion of state control mechanisms but also enhance the ability to operate anonymously, in a decentralized manner, and on a transnational scale. Within this framework, the article aims to identify emerging threats in the digital environment related to drug trafficking and associated crimes, construct a rigorous analytical model, and apply that model to propose response strategies for states and multilateral organizations.

Regarding the methodological approach, the study adopts a qualitative, exploratory perspective grounded in critical documentary analysis. It draws upon the theories of Johan Galtung and Elsa Blair Trujillo, which allow for an understanding of cyber violence beyond technical harm, emphasizing broader dimensions such as structural inequality, symbolic domination, and unresolved social conflicts. From this standpoint, digital threats are interpreted both in terms of their technical functioning and their deeper sociopolitical roots.

As a result, the research argues that the digital ecosystem has profoundly reshaped the nature of modern criminality, demanding a normative, ethical, and strategic renewal of cyber defense frameworks. It highlights the urgent need to establish effective international cooperation mechanisms based on shared intelligence, advanced surveillance, and comprehensive approaches that integrate social, economic, and political dimensions. In this way, cybersecurity is redefined as a systemic strategy aimed at protecting democracy, technological sovereignty, and fundamental rights in complex and constantly evolving environments.

**Keywords:** Cyberspace; Cyber defense; International cooperation; Drug trafficking; Violence

# [T1] Introducción

Durante los últimos años, el ciberespacio ha emergido como un ámbito prioritario en el que se entrecruzan factores relacionados con la seguridad nacional, el crimen organizado y el ejercicio del poder estatal y no estatal (Baldini & Kounelis, 2018; Brenner, 2011). Este espacio digital, originalmente concebido como una plataforma global de comunicación e intercambio de información, ha sido progresivamente adaptado por estructuras ilícitas incluidos carteles de droga, redes criminales transnacionales y actores armados no estatales con el fin de ampliar sus operaciones, diversificar sus métodos de acción y consolidar esquemas de dominio que trascienden los límites físicos y legales tradicionales (UNODC, 2021). En este contexto, el narcotráfico ha aprovechado las tecnologías emergentes no solo para optimizar su logística encubierta, sino también para blanquear capitales mediante activos digitales, captar colaboradores a través de redes sociales, infiltrarse en sistemas críticos y conectar con amenazas híbridas que difuminan la separación entre lo tangible y lo digital (Europol, 2022; Interpol, 2023).

Esta realidad plantea la necesidad de replantear los marcos analíticos clásicos en materia de seguridad internacional, pues la territorialización tradicional del crimen resulta insuficiente frente a un entorno virtual de rápida evolución. Se requiere una mirada holística que permita reconocer e interpretar las amenazas que se configuran dentro del ciberespacio, así como aquellas que, sin pertenecer exclusivamente a este dominio, se ven potenciadas por su instrumentalización tecnológica (FIP, 2021; Kaspersky Lab, 2022). Por ello, la presente investigación se enmarca en la pregunta orientadora: ¿Cómo identificar las amenazas presentes y emergentes, relacionadas con el narcotráfico y otras amenazas transnacionales en el ciberespacio? Esta interrogante permite examinar la transformación del delito en un entorno que opera bajo lógicas de descentralización, anonimato, cifrado y volatilidad informativa (Bada & Nurse, 2020).

El propósito central del artículo es desarrollar un análisis sistemático que contribuya a una mejor comprensión de las amenazas vinculadas al ciberespacio desde una perspectiva estructurada y multidimensional. En este marco, se proponen tres objetivos específicos que guían la investigación. El primero tiene como finalidad detectar y caracterizar las amenazas digitales relacionadas con el narcotráfico y con redes criminales transnacionales, tomando en cuenta el uso que hacen estas organizaciones de herramientas como redes privadas, plataformas de mensajería encriptada, sistemas de georreferenciación, y servidores descentralizados para evadir controles estatales (UNODC, 2021; Interpol, 2023). Este objetivo reconoce que dichas amenazas operan dentro de un ecosistema delictivo

que conecta actores diversos mediante dispositivos tecnológicos, vacíos normativos y flujos ilegales de capital (Brenner, 2011).

El segundo objetivo se enfoca en elegir un marco teórico y metodológico que permita realizar un análisis sistemático de los riesgos previamente identificados. Esta fase resulta indispensable para establecer criterios rigurosos de análisis, en sintonía con la complejidad, volatilidad y carácter no convencional de las amenazas cibernéticas actuales (Bada & Nurse, 2020). La literatura especializada en ciberseguridad, criminología internacional, inteligencia estratégica y sistemas predictivos de riesgo proporciona herramientas clave para estructurar una matriz analítica que clasifique las amenazas en función de variables como su alcance operativo, grado de sofisticación tecnológica, impacto institucional y articulación Inter actoral (Baldini & Kounelis, 2018; Europol, 2022). El enfoque teórico adoptado parte de postulados vinculados al análisis de redes ilícitas, conflictos híbridos y gobernanza del ciberespacio en contextos de fragilidad estatal (FIP, 2021).

El tercer y último objetivo consiste en aplicar el marco teórico seleccionado a las amenazas detectadas, diferenciando entre aquellas que se desarrollan exclusivamente en el ciberespacio —como los ciberataques, el uso de ransomware, el lavado digital de activos, o la manipulación algorítmica— y otras que, aunque tienen anclaje en el mundo físico, emplean herramientas digitales para reforzar su letalidad o eficacia operativa (Kaspersky Lab, 2022; UNODC, 2021). Esta aplicación busca no solo mapear patrones de comportamiento delictivo, sino también sentar las bases para la formulación de estrategias de prevención, respuesta e inteligencia colectiva que fortalezcan las capacidades de defensa estatal y cooperación multilateral ante un fenómeno de escala global (Interpol, 2023).

En síntesis, este artículo se alinea con una corriente investigativa que entiende el ciberespacio como un territorio estratégico en disputa, cuyo control representa una dimensión fundamental del poder contemporáneo frente al crimen organizado transnacional (Brenner, 2011; Europol, 2022). Al integrar perspectivas analíticas diversas, evidencia empírica actualizada y marcos conceptuales interdisciplinarios, esta investigación aspira a contribuir a una mejor comprensión de los desafíos que enfrentan los Estados, en particular en América Latina, donde la debilidad institucional y la sofisticación del delito cibernético se retroalimentan en un entorno de creciente incertidumbre (FIP, 2021; Baldini & Kounelis, 2018).

# [T1] Metodología

La investigación aquí desarrollada adoptó una estrategia metodológica cualitativa de naturaleza exploratoria, orientada a desentrañar las dinámicas profundas que vinculan el ciberespacio con las operaciones del narcotráfico y otras amenazas transnacionales. Esta elección se justifica por la complejidad inherente al objeto de análisis, el cual involucra múltiples escalas, actores y dimensiones que no pueden ser comprendidas a partir de datos puramente cuantitativos. En efecto, el fenómeno analizado requiere una lectura situada, capaz de interpretar las relaciones, interacciones y tensiones que se producen entre las estructuras criminales y las tecnologías digitales, reconociendo que estas no responden a lógicas deterministas sino a configuraciones emergentes y adaptativas.

Con este propósito, se llevó a cabo una revisión documental sistemática y crítica, que abarcó fuentes académicas, reportes técnicos, marcos doctrinales y publicaciones de referencia emitidas por organismos multilaterales especializados en seguridad y crimen transnacional, como Europol, Interpol y UNODC. Esta revisión no se limitó a recopilar información, sino que tuvo como objetivo construir un mapa interpretativo sobre los principales dispositivos, herramientas y estrategias digitales utilizadas por organizaciones criminales. En este proceso, se priorizó la triangulación de fuentes primarias y secundarias, con el fin de consolidar un análisis robusto, coherente y libre de sesgos interpretativos (Bada & Nurse, 2020; Europol, 2022; Interpol, 2023).

El objeto de análisis se delimitó a partir del examen de discursos y prácticas observadas en torno a la relación entre criminalidad organizada, tecnologías de información y contextos de conflicto híbrido. A partir de este corpus, se construyó un sistema de categorías analíticas que incluyó elementos como el anonimato digital, la instrumentalización de criptomonedas para el lavado de activos, la manipulación de plataformas sociales, el sabotaje digital a infraestructuras críticas, el uso de spyware y la creación de narrativas legitimadoras en entornos virtuales. La codificación temática se fundamentó en un enfoque transdisciplinar, con apoyo en los planteamientos teóricos de Johan Galtung y Elsa Blair Trujillo, quienes ofrecen herramientas conceptuales para abordar la violencia y el conflicto desde una mirada crítica y estructural.

Particularmente, el enfoque central para entender las amenazas digitales como expresiones de conflictos sociales no resueltos, que trascienden el plano técnico y se proyectan como manifestaciones de desigualdad, exclusión y concentración de poder. La violencia estructural, conceptualizada por Galtung (2003a), permitió examinar el trasfondo político y económico que facilita la proliferación de amenazas cibernéticas ligadas al narcotráfico. De esta manera, se superó la visión clásica centrada en

el ataque o la defensa tecnológica, para dar paso a una lectura crítica del entorno digital como espacio donde convergen contradicciones históricas y nuevas formas de dominación simbólica.

En un sentido complementario, el análisis de Blair Trujillo (2009) aportó una problematización del concepto de violencia, resaltando la necesidad de clarificar sus múltiples dimensiones —física, estructural, simbólica y tecnológica para evitar su utilización indiscriminada. Su enfoque permitió al equipo investigador identificar los matices entre distintos tipos de agresión digital, y cómo estas inciden no solo en la seguridad informática, sino también en los principios democráticos, la estabilidad institucional y la percepción pública de la legitimidad estatal.

La estrategia metodológica fue guiada por una lógica abductiva, que alternó momentos de inducción empírica con fases de deducción teórica. Esta dinámica permitió un diálogo constante entre los hallazgos documentales y el marco conceptual, favoreciendo una construcción progresiva del conocimiento. Más allá de describir amenazas, la investigación adoptó una postura reflexiva y crítica, en la que se analizaron también las limitaciones normativas, jurídicas y políticas que dificultan una respuesta articulada frente a las ciber amenazas contemporáneas.

Dado que este análisis se inscribe en el campo de la seguridad y la defensa nacional, se observó un estricto cumplimiento de los principios de ética investigativa. Todos los insumos empleados fueron obtenidos de fuentes públicas y accesibles, sin recurrir a materiales confidenciales ni comprometer protocolos de seguridad institucional. Asimismo, se garantizó la transparencia metodológica, trazabilidad de las fuentes y fidelidad epistemológica, conforme a los lineamientos establecidos por la Escuela Superior de Guerra "General Rafael Reyes Prieto".

En términos generales, esta propuesta metodológica permitió establecer una conexión sólida entre la pregunta de investigación referida a cómo identificar las amenazas actuales y emergentes vinculadas al narcotráfico y a fenómenos delictivos transnacionales en el entorno digital y los tres objetivos del análisis. El enfoque adoptado no pretende ofrecer soluciones unívocas, sino abrir caminos de interpretación, anticipación y formulación estratégica orientados al fortalecimiento de la ciberdefensa estatal y la cooperación internacional, en un escenario marcado por la complejidad, la incertidumbre y el cambio permanente.

## Amenazas en el ciberespacio asociadas al narcotráfico y amenazas transnacionales.

La comprensión integral de las amenazas asociadas al narcotráfico y a redes transnacionales en el ciberespacio requiere ampliar el enfoque más allá del análisis técnico o instrumental. Es necesario incorporar elementos de orden político, cultural, epistémico y social para abarcar la complejidad del fenómeno. El entorno digital ha expandido de forma significativa las capacidades operativas del crimen organizado, permitiéndole actuar con mayor discreción, rapidez y sin fronteras fijas. Esta evolución también ha modificado de forma profunda las dinámicas de los conflictos contemporáneos. Dentro de este escenario, es clave reconocer que los actores implicados en actividades ilícitas como el tráfico de drogas no se limitan a organizaciones criminales convencionales. En muchos casos, forman parte de redes transnacionales que combinan estructuras armadas, alianzas con sectores corruptos del poder, y agentes con conocimientos técnicos en ciber inteligencia y anonimato digital (Europol, 2022; Interpol, 2023).

El despliegue de herramientas como las redes privadas virtuales, sistemas de encriptación avanzada, plataformas de blockchain, canales de mensajería cifrada y activos digitales como las criptomonedas, ha facilitado una amplia gama de actividades criminales encubiertas. Estas tecnologías son utilizadas para ocultar operaciones logísticas, movilizar fondos, y coordinar acciones entre actores dispersos geográficamente, dificultando su detección por las autoridades competentes (UNODC, 2021; Zohar, 2015). Adicionalmente, se ha observado una tendencia creciente al uso de software malicioso como ransomware, ataques contra servicios públicos esenciales y manipulación de sistemas informáticos oficiales, con efectos directos en la estabilidad de las instituciones y la integridad del Estado (Kaspersky Lab, 2022).

Desde una perspectiva teórica, resulta pertinente incluir el enfoque de Johan Galtung, cuya propuesta sobre los conflictos enfatiza una mirada estructural e interdisciplinaria. Para este autor, los conflictos no son negativos en sí mismos, pero su escalamiento hacia la violencia refleja la incapacidad para ser gestionados adecuadamente (Calderón Concha, 2009). Bajo este prisma, el narcotráfico no debe analizarse únicamente como un delito, sino como una expresión sistémica de conflictos no resueltos que actúan en diversos niveles: desde lo individual hasta lo global (Galtung, 2003a). Esta lectura permite entender la violencia cibernética no solo como una agresión digital directa, sino como síntoma de tensiones geopolíticas, desigualdades económicas y fracturas sociales que se trasladan al ciberespacio.

En esta línea, el espacio digital puede interpretarse como un teatro de operaciones donde se manifiestan formas de violencia estructural. Esta última se entiende como la reproducción sistemática de condiciones de exclusión, dominación y negación de derechos, incluyendo el acceso a información, control de recursos o la participación política. Galtung distingue entre violencia directa, estructural y cultural, estableciendo un triángulo conceptual que permite interpretar cómo ciertos sistemas refuerzan dinámicas violentas, aunque no se expresen mediante el uso explícito de la fuerza (Galtung, 2003a; Calderón Concha, 2009). Aplicado al entorno digital, este enfoque visibiliza cómo los sistemas tecnológicos replican o amplifican desigualdades y conflictos que ya existían en el mundo analógico.

De forma complementaria, el aporte teórico de Elsa Blair Trujillo contribuye a problematizar el concepto mismo de violencia, advirtiendo sobre su uso excesivo, ambiguo y poco operativo. Blair sostiene que el término ha sido empleado para designar fenómenos muy distintos desde crímenes individuales hasta guerras lo cual impide una conceptualización clara y coherente (Blair Trujillo, 2009). Este señalamiento es especialmente relevante para el análisis de amenazas digitales, donde el uso indiscriminado del concepto de violencia puede llevar a confusiones al no diferenciar entre actos simbólicos, estructurales o tecnológicos. En consecuencia, para entender la violencia asociada al ciberespacio se necesita una conceptualización que clasifique con precisión los distintos tipos de agresión y sus implicaciones institucionales.

La violencia en el ciberespacio también puede manifestarse como una forma de dominación cultural. La propagación de discursos que glorifican el narcotráfico, el reclutamiento digital de jóvenes en situación de vulnerabilidad, o el uso de causas sociales como fachada para actividades criminales, constituyen expresiones simbólicas que consolidan imaginarios de poder, desigualdad y exclusión (Galtung, 2003c; Blair Trujillo, 2009). Aunque menos visibles que los ciberataques directos, estas prácticas erosionan el tejido institucional y social, actuando como formas encubiertas de violencia cultural.

Tanto Galtung como Blair coinciden en la necesidad de abordar el fenómeno desde una óptica crítica e interdisciplinaria. El primero propone la transformación de los conflictos a través de su metodología Transcended, basada en la creatividad, el entendimiento mutuo y la solución pacífica de contradicciones. Esta visión enfatiza la importancia de intervenir en las causas estructurales que generan violencia y no limitarse a sus manifestaciones visibles (Galtung, 2003a). Por su parte, Blair insiste en que cualquier intento de conceptualizar la violencia debe estar enraizado en su contexto

histórico, político y discursivo, y alerta contra los enfoques normativos que ignoran la complejidad empírica del fenómeno (Blair Trujillo, 2009).

En síntesis, identificar las amenazas del ciberespacio ligadas al narcotráfico exige una doble mirada: por un lado, un análisis técnico que reconozca las herramientas utilizadas por los actores delictivos, y por otro, una interpretación estructural que visibilice los conflictos sociales que estas prácticas reproducen o encubren. La visión de Galtung permite entender que detrás de cada forma de violencia digital se oculta un entramado conflictivo más profundo, mientras que Blair recuerda la necesidad de un uso riguroso y crítico de los conceptos para no trivializar fenómenos de gran impacto. En conjunto, estos enfoques permiten trazar una ruta más sólida para diagnosticar, interpretar y eventualmente mitigar las ciber amenazas de carácter transnacional.

**Narcotráfico como eje estructurante del crimen digital transnacional**

El narcotráfico se dispersa en redes digitales donde el ciberespacio potencia su alcance. Los cárteles han adoptado una "plataformización del delito", usando infraestructura digital para planear, ejecutar y expandir sus acciones (UNODC, 2021; Europol, 2022). Esto les permite consolidar economías ilegales, optimizar rutas de distribución y controlar territorios, con apoyo de tecnología de la información. A diferencia de otros delitos, el narcotráfico mezcla grandes recursos financieros, estructuras de poder y estrategias híbridas que le otorgan estatus transnacional. No solo amenaza la seguridad interna de los países; también pone en jaque la soberanía tecnológica, la integridad institucional y el manejo de datos en América Latina (González & Rivas, 2021). El ciberespacio se ha convertido en un "corredor invisible" por donde circulan órdenes, criptoactivos, campañas de propaganda, chantajes y reclutamiento.

**1. Lavado de dinero con criptoactivos y plataformas descentralizadas**

Las criptomonedas y el blockchain ofrecen anonimato, descentralización y opacidad. Eso ha permitido a los narcos mover grandes sumas sin depender de bancos formales (Zohar, 2015; UNODC, 2021). Usan intercambios P2P, mezcladores (mixers) y plataformas DeFi para transformar sus ganancias en activos virtuales y burlar la fiscalización.

El informe de la UNODC (2021) señala que el narco ya usa Bitcoin, Monero y otras criptomonedas con alta opacidad. Incluso existen plataformas especializadas en "crypto laundering", donde se mezclan transacciones criminales con otras legítimas, borrando el rastro ilícito. Este panorama pone sobre la mesa la necesidad de una cooperación global para regular los activos digitales.

La norma ISO/IEC 27005 (2018) recomienda que los gestores de riesgo digital consideren flujos virtuales, suplantación de identidad y transacciones no declaradas. Además, Europol (2022) alerta que los cárteles han incorporado desarrolladores, hackers y hasta plataformas de trading ilegal para construir una economía paralela que opera al margen de la legalidad.

**2. Manipulación digital para reclutamiento y control territorial**

Otro frente clave es la manipulación informativa en redes y apps encriptadas para reclutar, consolidar poder y construir legitimidad. A través de contenidos que enaltecen la "vida narco", promesas de protección o ayuda económica, las organizaciones delictivas lanzan campañas digitales cargadas de resonancia emocional (Castells, 2012; Interpol, 2023).

Galtung (2003c) lo define como violencia cultural digital: se normaliza la dominación criminal usando símbolos, lenguaje y discursos que maquillan la ilegalidad. Así, el narcotráfico no solo se ve rentable, también como alternativa de vida frente al abandono estatal.

Interpol (2023) informa un aumento notable en el uso de Telegram, WhatsApp y TikTok para reclutar encubiertamente y distribuir instrucciones en tiempo real. Estas plataformas cifradas dificultan el monitoreo y permiten organizar operaciones sin exponer físicamente a los líderes. Además, emplean bots y cuentas falsas para difundir propaganda narco, desinformación política o desprestigio institucional, aumentando la desconfianza pública.

Para enfrentar esto, la ciberseguridad debe ir más allá de proteger infraestructuras. Como señala Blair Trujillo (2009), la violencia simbólica puede ser tan dañina como un ciberataque directo. Por eso hace falta resiliencia cultural, alfabetización mediática y contranarrativas claras desde las autoridades.

Lo que se está viendo no es un delito digital más, es una convergencia compleja de prácticas financieras, simbólicas y tecnológicas que fortalecen estructuras criminales. El uso de criptoactivos para el lavado y la manipulación mediática para el control son dos caras de esta realidad y requieren respuestas integrales: inteligencia digital, cooperación internacional y cambios estructurales. Como advierte Galtung (2003a), si no enfrentamos el problema de raíz, este tiende a reinventarse y volverse más agresivo. Reconocer estas amenazas es el primer paso para atacarlas desde su origen, no solo sus síntomas tecnológicos.

## Marco de referencia para realizar el estudio sistemático de las amenazas identificadas.

La elección de un marco de referencia metodológico adecuado para analizar de manera sistemática las amenazas derivadas del narcotráfico y otros riesgos transnacionales que se manifiestan en el ciberespacio, representa una decisión de gran importancia estratégica. Las organizaciones criminales dedicadas al narcotráfico han adoptado nuevas formas de operación digital, utilizando canales cifrados, tecnologías de anonimato y herramientas propias del cibercrimen, lo que hace necesario repensar los enfoques clásicos de seguridad. Por tanto, resulta esencial estructurar un modelo de análisis que permita clasificar, interpretar y comprender estas amenazas, considerando su impacto en la seguridad nacional, su vínculo con redes internacionales delictivas y su efecto sobre infraestructuras críticas.

En ese sentido, un referente relevante es el paradigma de seguridad integral propuesto por la Organización de Estados Americanos (OEA), el cual redefine el concepto de seguridad desde una visión multidimensional que incorpora variables sociales, económicas, políticas y tecnológicas (OEA, 2011). Esta perspectiva facilita un abordaje más completo del narcotráfico digital, reconociéndolo como un fenómeno multifacético que desborda lo puramente militar. Asimismo, especialistas como Bayuk y colaboradores (2012) proponen una visión más amplia de la ciberseguridad, destacando que debe articularse con políticas de gobernanza, gestión de riesgos y resiliencia institucional para afrontar con eficacia las amenazas cibernéticas de carácter complejo.

Cabe destacar que no existe un único marco normativo o metodológico que permita abordar de forma absoluta las amenazas cibernéticas transnacionales. Una alternativa ampliamente utilizada en entornos de defensa es el análisis de amenazas persistentes avanzadas (APT), que facilita la identificación de patrones sostenidos de actividad maliciosa a largo plazo, muchos de los cuales son utilizados por estructuras criminales para evadir la detección estatal (Zetter, 2014). A este enfoque se le pueden incorporar elementos teóricos de la Escuela de Copenhague, particularmente la Teoría de la Seguridad Ampliada formulada por Buzan y Wæver (2003), que permite examinar las amenazas desde esferas no convencionales como lo cultural, lo económico y lo ambiental, aportando una visión holística al fenómeno del cibercrimen relacionado con el narcotráfico.

Paralelamente, es fundamental considerar marcos normativos de gestión del riesgo en sistemas digitales, como el desarrollado por la norma ISO/IEC 27005 (Organización Internacional de

Normalización, 2018), que orienta la identificación, evaluación y tratamiento de riesgos en infraestructuras informáticas. Su estructura puede adaptarse a contextos gubernamentales o militares, permitiendo incorporar principios de ciberinteligencia en la evaluación de amenazas. En esa dirección, investigaciones como las de Craigen, Diakun-Thibault y Purse (2014) recomiendan emplear marcos internacionales estandarizados para facilitar la colaboración interinstitucional, la interoperabilidad entre sistemas de defensa y la generación de respuestas unificadas frente a ciberamenazas.

Por lo tanto, para este estudio se propone la integración de un modelo híbrido que combine el enfoque de seguridad multidimensional de la OEA, la metodología APT para el rastreo de amenazas organizadas y la gestión técnica del riesgo contemplada en la ISO/IEC 27005. Esta combinación metodológica permitirá desarrollar un análisis riguroso y estructurado, abordando las amenazas desde una óptica estratégica, técnica y social. Al consolidar estas perspectivas se busca generar una base sólida para diseñar políticas públicas de ciberdefensa más efectivas, fortalecer los marcos de cooperación internacional y anticiparse a los riesgos que surgen de la convergencia entre crimen organizado y ciberespacio

Tabla 1

| **Nombre del Enfoque o Marco** | **Caracterización General** | **Aplicabilidad al Estudio de Amenazas Cibernéticas** |
|---|---|---|
| Seguridad Multidimensional (OEA) | Integra variables sociales, políticas, económicas, culturales y tecnológicas. Requiere coordinación interinstitucional. | Permite abordar el narcotráfico digital como fenómeno complejo más allá del ámbito militar. |
| Ciberseguridad Integral (Bayuk et al.) | Propone un enfoque holístico que vincula políticas de gobernanza, gestión de riesgos y resiliencia. | Aporta lineamientos estratégicos para la formulación de políticas públicas de ciberdefensa. |
| APT – Amenazas Persistentes Avanzadas | Modelo técnico-operativo para rastrear actividades maliciosas sofisticadas y sostenidas. | Útil para identificar amenazas organizadas con alta capacidad tecnológica. |
| Teoría de la Seguridad Ampliada (Escuela de Copenhague) | Amplía el concepto de seguridad a dimensiones no tradicionales (cultural, económica, ambiental). | Favorece un análisis interseccional del cibercrimen en contextos frágiles. |
| ISO/IEC 27005 | Norma internacional para gestión de riesgos en seguridad de la información. | Aporta criterios técnicos estandarizados para identificar, evaluar y tratar amenazas. |
| Análisis Crítico de Redes Criminales Transnacionales | Estudia interconexiones entre actores ilícitos, flujos financieros y tecnología. | Fundamenta el análisis estructurado de vínculos entre cibercrimen y narcotráfico. |
| Violencia estructural y cultural (Galtung) | Propone comprender la violencia como resultado de desigualdades | Permite identificar la raíz sociopolítica de amenazas digitales persistentes. |

| | | |
|---|---|---|
| | sistémicas y dominación simbólica. | |
| Conceptualización crítica de la violencia (Blair Trujillo) | Advierte sobre el uso indiscriminado del concepto de violencia. Distingue entre tipos de agresión. | Clarifica los límites y alcances de la violencia cibernética como fenómeno diferenciado. |
| Marco de capacidades cibernéticas (Bada & Nurse) | Describe desafíos y prácticas para el desarrollo de capacidades en ciberseguridad. | Apoya el diagnóstico institucional sobre capacidades de respuesta ante amenazas. |
| Gobernanza Cibernética y Riesgo Estratégico (Craigen et al.) | Plantea un marco de referencia unificado para la definición de ciberseguridad y su gestión. | Contribuye a la interoperabilidad institucional en contextos de defensa y cooperación. |

Fuente Propia

La incorporación y articulación de diversos marcos de referencia permite configurar una perspectiva mixta que examine las amenazas cibernéticas vinculadas al narcotráfico desde distintos niveles: estratégico, técnico, regulatorio y sociopolítico. Esta diversidad metodológica no solo potencia la comprensión del fenómeno, sino que también proporciona fundamentos robustos para la formulación de políticas públicas, la consolidación de alianzas internacionales y la identificación preventiva de posibles riesgos. Al asumir esta visión integradora, el estudio se posiciona dentro de una línea avanzada de investigación en ciberseguridad, en la cual los enfoques interdisciplinares se vuelven esenciales para abordar problemáticas complejas.

La tabla se orienta hacia la construcción de un marco teórico y metodológico que permita abordar de forma rigurosa las amenazas cibernéticas vinculadas al narcotráfico, constituyéndose en una iniciativa investigativa de notable relevancia dentro del ámbito de la ciberseguridad estratégica. La naturaleza compleja del fenómeno obliga a trascender las aproximaciones técnico-operativas tradicionales, apostando por una estructura conceptual de carácter transdisciplinario que incorpore variables sociopolíticas, institucionales y regulatorias. En consecuencia, el autor opta por una metodología híbrida que articula normativas internacionales, esquemas técnicos de detección de amenazas persistentes y teorías críticas sobre el poder y la violencia. Esta convergencia metodológica permite configurar una base analítica sólida para interpretar las amenazas digitales no como incidentes aislados, sino como manifestaciones de procesos sociales más amplios, sostenidos por desigualdades históricas, debilidad institucional y mecanismos de dominación simbólica adaptados al entorno digital.

Uno de los aspectos más destacados de este enfoque es la incorporación del paradigma de seguridad multidimensional promovido por la Organización de Estados Americanos (OEA), el cual habilita una mirada más comprehensiva de la ciberseguridad al ir más allá de la defensa de infraestructuras

críticas. Este modelo plantea que amenazas como el narcotráfico digital son fenómenos complejos alimentados por dinámicas como la exclusión estructural, la corrupción institucional y la carencia de gobernanza eficaz, lo que exige respuestas que involucren múltiples sectores del Estado y de la sociedad. Asimismo, la inclusión del enfoque de amenazas persistentes avanzadas (APT), propio del ámbito de la inteligencia estratégica, añade un componente técnico crucial al posibilitar la detección de patrones delictivos sostenidos, tales como el uso sistemático de malware, la manipulación de criptoactivos o la infiltración de redes logísticas a través de técnicas sofisticadas como el spear phishing. Esta herramienta se vuelve indispensable para mapear estructuras criminales descentralizadas, adaptativas y de larga duración, que mutan conforme a los entornos regulatorios y tecnológicos.

El uso de la norma ISO/IEC 27005 refuerza este andamiaje metodológico al ofrecer un marco normativo estandarizado para la gestión de riesgos cibernéticos. Su implementación en escenarios estatales y de seguridad nacional permite fortalecer las capacidades técnicas institucionales, garantizar la interoperabilidad entre sistemas y proporcionar trazabilidad a las decisiones estratégicas. Además, dicha norma traduce el análisis conceptual en instrumentos concretos de gestión como matrices de riesgo, modelos de contingencia o protocolos de alerta. No obstante, el principal valor del objetivo radica en la fusión de esta infraestructura técnica con enfoques críticos propuestos por académicos como Johan Galtung y Elsa Blair Trujillo. En particular, la noción de violencia estructural formulada por Galtung permite reinterpretar las amenazas digitales no únicamente como ataques informáticos, sino como la cristalización de condiciones estructurales de exclusión y desigualdad, instrumentalizadas por redes delictivas para consolidar poder, reclutar adeptos y debilitar sistemas institucionales vulnerables.

El aporte de Blair Trujillo introduce una advertencia epistemológica crucial al señalar la necesidad de precisar los alcances del concepto de violencia en el ciberespacio. La autora advierte que el uso indiscriminado del término puede provocar errores analíticos y distorsionar la jerarquización de riesgos, desatendiendo aquellos más profundos y menos visibles. Esta advertencia resulta clave en contextos donde la violencia simbólica y cultural opera mediante estrategias de seducción digital, glorificación del delito en redes sociales o instrumentalización narrativa de causas sociales, con efectos disruptivos sobre la legitimidad estatal y la percepción de seguridad ciudadana. Tales fenómenos, aunque no impliquen agresiones cibernéticas directas, configuran escenarios de conflicto que escapan a los marcos de intervención tradicionales.

La lógica abductiva que estructura este segundo objetivo constituye otro de sus aportes metodológicos sobresalientes. Al combinar elementos empíricos con constructos teóricos de forma iterativa, se facilita una comprensión progresiva del objeto de estudio, adaptada a la fluidez e imprevisibilidad del ecosistema digital. Esta estrategia es coherente con lo planteado por Craigen, Diakun-Thibault y Purse (2014), quienes sostienen que los análisis en ciberseguridad deben ser flexibles, dinámicos e interoperables, dada la naturaleza evolutiva de las amenazas. En esta línea, el modelo propuesto permite construir hipótesis interpretativas robustas sin incurrir en reduccionismos tecnológicos, fortaleciendo tanto la validez interna del estudio como su aplicabilidad en el diseño de políticas públicas, estrategias de defensa nacional y marcos de cooperación internacional.

El segundo objetivo no solo destaca por su sofisticación analítica, sino también por su orientación pragmática. Más allá de elaborar una crítica del estado del arte, la investigación propone mecanismos de intervención concretos, como sistemas de alerta temprana colaborativa, estrategias de disuasión digital o campañas comunicativas institucionales orientadas a neutralizar el impacto simbólico de las organizaciones criminales. La incorporación de elementos teóricos derivados de la Escuela de Copenhague, particularmente su enfoque sobre seguridad ampliada extiende el alcance del análisis al considerar otras dimensiones relevantes como la seguridad ambiental, económica y cultural. Esta perspectiva resulta esencial en el caso latinoamericano, donde el narcotráfico está íntimamente relacionado con procesos de explotación territorial, captura institucional y marginación de comunidades vulnerables.

El abordaje analítico del ciberespacio y de los desafíos que emergen en su interior exige la formulación de un marco conceptual que desborde las interpretaciones reduccionistas centradas únicamente en la dimensión tecnológica o instrumental de las amenazas. Lejos de ser una mera infraestructura de redes, protocolos y dispositivos, el ciberespacio constituye hoy un campo de acción estratégica, simbólica y política, en el cual se redefine el ejercicio del poder, la soberanía, la seguridad y los derechos ciudadanos (Cavelty, 2014). Su configuración responde a dinámicas altamente complejas, que incluyen asimetrías en el acceso, concentración de capacidades técnicas, conflictos regulatorios transnacionales, disrupciones institucionales y nuevas formas de exclusión. Por esta razón, el análisis del entorno cibernético demanda una arquitectura teórica que sea capaz de integrar dimensiones estructurales, discursivas, normativas, tecnológicas y éticas.

### 1. El ciberespacio como construcción sociotécnica

En primer lugar, es necesario concebir el ciberespacio como una construcción sociotécnica, es decir, como un entorno configurado no solo por máquinas y algoritmos, sino también por relaciones sociales, intereses económicos, estructuras institucionales y marcos culturales. Esta perspectiva, sustentada en la teoría actor-red y en la sociología de la tecnología, permite visualizar que cada dispositivo, cada plataforma y cada infraestructura digital lleva consigo una serie de valores, lógicas de control y jerarquías sociales (Latour, 2005; Castells, 2012). De este modo, no se trata únicamente de analizar "tecnologías neutras", sino de entender cómo estas tecnologías participan activamente en la organización del mundo social, en la mediación de los conflictos y en la producción de subjetividades.

Desde este enfoque, el ciberespacio no es un "lugar" o "medio" pasivo, sino un territorio dinámico de disputa donde se articulan múltiples formas de gobernanza, resistencia, vigilancia y producción simbólica. La lógica de plataformas, por ejemplo, redefine las relaciones entre actores públicos y privados, y otorga a las grandes corporaciones tecnológicas un poder sin precedentes sobre los flujos de información, la visibilidad pública y la regulación de los discursos (Zuboff, 2019). Por tanto, cualquier marco teórico robusto debe partir de la comprensión de esta sociotécnica del poder digital.

### 2. Seguridad digital como bien público transnacional

Un segundo elemento fundamental es la concepción de la seguridad digital como un bien público transnacional, que requiere mecanismos coordinados de protección, regulación y cooperación. En un entorno interconectado y descentralizado, los riesgos cibernéticos trascienden las fronteras estatales y desafían los esquemas tradicionales de seguridad basados en la territorialidad. Esta realidad ha impulsado a organismos multilaterales, como la OEA, la ONU y la Unión Europea, a promover marcos normativos comunes y estrategias compartidas, bajo la premisa de que la ciberseguridad debe construirse de forma colaborativa, basada en la confianza mutua, la interoperabilidad técnica y la solidaridad normativa (OEA, 2020; ENISA, 2023).

Este enfoque plantea que la seguridad cibernética debe ser entendida en términos más amplios que la simple protección de infraestructuras críticas. Implica también garantizar derechos fundamentales como la privacidad, la libertad de expresión, la protección de datos personales y el acceso a la información. Así, se inscribe dentro de una noción de seguridad humana integral, donde los riesgos

digitales no se limitan a lo técnico, sino que afectan directamente la vida, dignidad y agencia de las personas en entornos altamente digitalizados.

### 3. Capacidades cibernéticas y madurez institucional

En tercer lugar, el análisis teórico debe incorporar la noción de capacidades cibernéticas como indicador clave del nivel de preparación y resiliencia de un Estado o institución frente a desafíos digitales. Esta perspectiva, desarrollada por Bada y Nurse (2020), propone que la capacidad cibernética es un constructo multidimensional que incluye no solo infraestructura tecnológica, sino también marcos legales, recursos humanos, cultura de ciberhigiene, redes de colaboración y mecanismos de respuesta articulada. En este sentido, la evaluación de amenazas no puede desvincularse de una lectura crítica sobre las capacidades institucionales existentes para afrontarlas.

Este modelo permite identificar tanto fortalezas como brechas estructurales, visibilizando que la ciberseguridad es, ante todo, una función de gobernanza pública sostenida. De hecho, muchas de las vulnerabilidades más críticas no derivan de la falta de tecnología, sino de la ausencia de estrategias, la descoordinación interinstitucional o la falta de voluntad política. En este marco, el desarrollo de capacidades implica invertir en formación, establecer marcos de políticas públicas coherentes, construir alianzas internacionales y fomentar una cultura de seguridad digital que permee todos los niveles de la sociedad.

### 4. Teoría crítica de la securitización digital

Un cuarto componente clave lo constituye la teoría crítica de la securitización digital, la cual ofrece herramientas para problematizar cómo ciertos actores definen qué es una amenaza, con qué discursos lo hacen, qué intereses están en juego y qué consecuencias políticas se derivan de tales definiciones. Inspirada en la Escuela de Copenhague (Buzan & Wæver, 2003), esta teoría sostiene que la seguridad no es una categoría objetiva, sino una construcción social resultado de procesos discursivos. Aplicada al entorno cibernético, esta mirada permite evidenciar cómo ciertas narrativas de "ciberpeligro" pueden usarse para justificar restricciones a los derechos, vigilancia masiva, militarización digital o monopolización del conocimiento técnico.

En este sentido, se advierte sobre el riesgo de que la ciberseguridad se convierta en un campo hegemonizado por intereses corporativos o estatales que excluyen a la ciudadanía del debate público. Por eso, autores como Dunn Cavelty (2014) defienden una estrategia de seguridad digital

democrática, inclusiva y transparente, que no sacrifique la libertad por la promesa de protección, y que contemple principios éticos, control ciudadano y acceso equitativo al conocimiento técnico.

**5. Perspectiva sistémica y complejidad del entorno digital**

Finalmente, el marco teórico se enriquece con un enfoque sistémico y complejo del entorno digital, que permite comprender las amenazas no como eventos aislados, sino como el resultado de interacciones múltiples, retroalimentadas y no lineales entre factores técnicos, humanos, institucionales y culturales (Rid, 2013). Este enfoque asume que el comportamiento de los sistemas digitales es emergente, incierto y dinámico, lo cual exige metodologías de análisis abductivo, pensamiento estratégico flexible y esquemas de anticipación adaptativa.

La complejidad del ecosistema cibernético implica que cualquier modelo analítico debe integrar diversas escalas de observación (local, nacional, internacional), así como diferentes niveles de análisis (infraestructural, simbólico, normativo). Solo de este modo será posible generar diagnósticos realistas, diseñar estrategias de respuesta proporcionales y construir políticas públicas que respondan a los desafíos estructurales del entorno digital contemporáneo.

En conclusión, este segundo objetivo representa una propuesta metodológica de alta complejidad, tanto en el plano conceptual como operativo, que se distingue por su capacidad integradora, su apertura epistemológica y su orientación a la acción estratégica. Al articular herramientas técnicas, normativas internacionales y perspectivas críticas, se logra un análisis multidimensional de las amenazas cibernéticas, capaz de generar insumos valiosos para la formulación de políticas públicas, el fortalecimiento institucional y la consolidación de esquemas de defensa cibernética multinivel frente a los desafíos que emergen de la convergencia entre crimen organizado y tecnología digital.

## Aplicar el marco de referencia del estudio sistemático a las amenazas encontradas, tanto aquellas restringidas al ciberespacio y las relacionadas con el mismo.

La aplicación del marco de referencia del estudio sistemático a las amenazas identificadas ya sea las que se desarrollan exclusivamente en el ciberespacio o las que tienen algún componente digital, facilita una comprensión más profunda de la estructura y dinámica del crimen organizado transnacional, con especial atención al narcotráfico y sus transformaciones tecnológicas. Este enfoque metodológico se sustenta en tres pilares fundamentales: la seguridad multidimensional de la OEA, la evaluación técnica mediante APT (Amenazas Persistentes Avanzadas) y la gestión de riesgos conforme a la norma ISO/IEC 27005:2018. Además, incorpora una mirada crítica desde la teoría de la violencia estructural de Johan Galtung y la conceptualización de violencia digital de Elsa Blair Trujillo. La combinación de estas perspectivas permite integrar aspectos técnicos, institucionales y simbólicos con coherencia, anticipar escenarios y fortalecer la toma de decisiones estratégicas en ciberseguridad.

Con esta integración metodológica, es posible caracterizar amenazas puramente digitales, como ataques DDoS, ransomware dirigido a entidades públicas, manipulación algorítmica para desinformación o software espía que penetra redes institucionales. Según Zetter (2014), estas amenazas siguen lógicas de persistencia técnica avanzada, superando las capacidades tradicionales de los Estados: diseñadas para permanecer ocultas, recolectar datos y deteriorar infraestructura crítica. Gracias a la metodología APT se pueden detectar patrones de actividad maliciosa sostenida, evaluar su grado de sofisticación y trazar rutas de ataque empleadas por organizaciones criminales o actores estatales. Esto resulta imprescindible para prever futuras amenazas y construir defensas adaptativas, no reactivas.

También emergen amenazas híbridas que combinan lo presencial con herramientas digitales: reclutamiento online por grupos delictivos, uso de plataformas cifradas para coordinar acciones criminales y producción de propaganda mediante narrativas visuales en redes sociales. Interpol (2023) y Europol (2022) documentan cómo estas estructuras emplean cifrado, criptomonedas y redes sociales para operar de forma global, difusa y descentralizada, lo que complica su detección legal tradicional. El informe IOCTA 2022 de Europol resalta que estas organizaciones han montado plataformas

especializadas para lavado de dinero digital, tráfico de información sensible y venta de sustancias ilegales, mucho operando en la dark web con autenticación doble y cifrado extremo.

Según el modelo de seguridad multidimensional de la OEA (2011), estas amenazas deben evaluarse no solo por su potencial disruptivo inmediato, sino también por su impacto en la gobernabilidad, los derechos humanos, la estabilidad institucional y la seguridad humana. En este sentido, la seguridad digital trasciende la protección de sistemas informáticos: se convierte en defensa integral del Estado democrático. Por ello, la respuesta debe involucrar a múltiples actores: inteligencia, justicia, fuerzas armadas, educación y sociedad civil, siguiendo principios de cooperación, transparencia y gobernanza compartida.

La norma ISO/IEC 27005:2018 aporta criterios estandarizados para identificar, evaluar y gestionar riesgos digitales, permitiendo crear matrices que estiman la probabilidad, impacto sobre activos críticos y capacidades de respuesta institucional. Esto orienta la priorización de amenazas y la asignación de recursos. En entornos gubernamentales con capacidades desiguales, este enfoque traduce la "resiliencia cibernética" en indicadores medibles, protocolos de contingencia y sistemas de alerta temprana.

Conectar estas aproximaciones técnicas con las visiones críticas permite redefinir nuestra comprensión de las amenazas. Para Galtung (2003a), la violencia incluye formas estructurales de exclusión y dominación, no solo daños visibles. En el ciberespacio, ello expone cómo las tecnologías digitales pueden perpetuar desigualdades, marginar poblaciones y facilitar el control encubierto de actores ilícitos. Blair Trujillo (2009) advierte que una definición imprecisa de violencia digital puede conducir a respuestas desproporcionadas, invisibilizando amenazas simbólicas o normativas que afectan la legitimidad democrática. Así, aplicar un enfoque sistemático y crítico permite distinguir entre amenazas tecnológicas, simbólicas o estructurales y responder con estrategias adecuadas.

Este enfoque también identifica brechas importantes en las capacidades cibernéticas de las instituciones. Según Bada y Nurse (2020), la madurez en ciberseguridad no depende solo de recursos tecnológicos, sino de leyes actualizadas, personal capacitado, sistemas claros y una cultura organizacional orientada a la protección digital. Muchas amenazas no provienen solo de su naturaleza técnica, sino de las debilidades institucionales: fallas en interoperabilidad, fragmentación de competencias y falta de articulación entre agencias estatales representan vulnerabilidades críticas.

Finalmente, este modelo no busca clasificar amenazas de forma estática, sino promover una lectura dinámica, anticipativa y multiescalar de los riesgos emergentes. En un entorno digital que cambia velozmente, con amenazas que evolucionan según el contexto sociopolítico, este marco debe entenderse como una herramienta viva, sujeta a revisión y enriquecimiento continuo mediante el diálogo entre teoría crítica, evidencia empírica y práctica institucional. Como señala Dunn Cavelty (2014), el mayor riesgo en ciberseguridad no es la falta de tecnología, sino la carencia de reflexión estratégica sobre las condiciones que habilitan las amenazas. Así, este enfoque busca contribuir metodológicamente a afrontar los desafíos que plantea la convergencia entre crimen organizado, tecnologías emergentes y gobernabilidad democrática.

| Tipo de amenaza | Ejemplos concretos | Marco aplicado | Recomendaciones |
|---|---|---|---|
| **1. Amenazas técnicas (exclusivas del ciberespacio)** | Ciberataques y explotación de vulnerabilidades:• Malware especializado (troyanos, keyloggers, spyware) para infiltración en redes gubernamentales y militares.• Ransomware dirigido a entidades de seguridad y servicios públicos esenciales, buscando extorsión y paralización de operaciones.• Ataques DDoS contra portales institucionales, sistemas de control fronterizo y plataformas de inteligencia.Ciberfraude y manipulación digital:• Spear phishing para obtención de credenciales críticas de funcionarios estratégicos.• Ingeniería social avanzada apoyada en análisis de metadatos y OSINT.Criminalidad financiera digital:• Lavado de activos mediante criptomonedas (Bitcoin, Monero) usando mixers, exchanges P2P y plataformas DeFi.• Uso de | Técnicos y normativos:• APT – Amenazas Persistentes Avanzadas (Zetter, 2014) como metodología para rastreo y caracterización de ataques sofisticados y prolongados.• ISO/IEC 27005:2018 para la identificación, evaluación, tratamiento y monitoreo de riesgos en seguridad de la información.• Seguridad tecnológica del modelo de Seguridad Multidimensional (OEA, 2011) para integración institucional.Operativos y de inteligencia:• Principios de ciberinteligencia aplicada según Craigen et al. (2014) para análisis predictivo.• Modelos de análisis forense digital en entornos militares.Doctrinales:• Integración con protocolos de defensa cibernética y manuales técnicos de Fuerzas Militares. | Operativas y preventivas:1. Implementar sistemas de detección y respuesta temprana (SIEM, SOC, CERT gubernamentales) con interoperabilidad internacional.2. Capacitar a personal de inteligencia, defensa y justicia en APT, análisis forense digital y respuesta ante incidentes críticos.3. Fortalecer el uso de ISO/IEC 27005 para priorización de riesgos, asignación de recursos y planes de continuidad operativa.4. Establecer alianzas con Europol, Interpol y UNODC para intercambio de inteligencia técnica en tiempo real.5. Desarrollar capacidades de ciberinteligencia ofensiva para rastrear, infiltrar y desmantelar infraestructuras criminales.6. Simular escenarios de ciberataque a nivel institucional para evaluar resiliencia y tiempos de respuesta.7. Promover encriptación robusta y control de accesos para activos |

| | | | |
|---|---|---|---|
| | blockchain para transacciones opacas y sin trazabilidad.Amenazas tecnológicas avanzadas:• Explotación de vulnerabilidades "zero-day" en sistemas críticos.• Manipulación algorítmica y de inteligencia artificial para evasión de detección.• Infiltración en SCADA/ICS para afectar infraestructura crítica (energía, transporte, telecomunicaciones). | | estratégicos, con segmentación de redes críticas. |

| | | | |
|---|---|---|---|
| **2. Amenazas híbridas (relacionadas con el ciberespacio)** | Propaganda y control simbólico:• Narrativas digitales que glorifican la cultura narco y normalizan la violencia (videos, música, memes, transmisiones en vivo).• Uso de causas sociales como fachada para justificar la actividad ilícita.Reclutamiento y coordinación operativa:• Captación de jóvenes en situación de vulnerabilidad mediante promesas económicas o de protección.• Uso de plataformas cifradas (Telegram, WhatsApp, Signal) para coordinar acciones presenciales.Desinformación y manipulación social:• Campañas de desprestigio contra autoridades e instituciones de seguridad.• Creación de cuentas falsas y bots para amplificar mensajes y polarizar comunidades.Crimen transnacional facilitado digitalmente:• Coordinación de rutas y logística de narcotráfico mediante sistemas de georreferenciación.• Venta encubierta de armamento o precursores químicos en la dark web.• Intercambio de inteligencia criminal entre grupos transnacionales a través de servidores seguros y descentralizados. | Teóricos y críticos:• Johan Galtung (2003a, 2003c) – violencia estructural y cultural: explica cómo la tecnología reproduce desigualdades y refuerza el control criminal.• Elsa Blair Trujillo (2009) – conceptualización crítica de la violencia: clasifica amenazas simbólicas, estructurales y tecnológicas.Normativos y estratégicos:• Seguridad humana e institucional (OEA, 2011) como dimensión integral de protección ciudadana e institucional.• Teoría de la seguridad ampliada (Buzan & Wæver, 2003) para abordar dimensiones no militares (cultural, económica, social).Operativos:• Protocolos de contranarrativa y campañas de alfabetización digital.• Uso de ciberinteligencia para identificación de redes de influencia criminal. | Preventivas y de resiliencia social:1. Diseñar programas de alfabetización mediática y digital que enseñen a identificar propaganda y desinformación.2. Generar contranarrativas institucionales y comunitarias que desacrediten el atractivo simbólico del narcotráfico.3. Implementar unidades especializadas en ciberpsicología y análisis de comportamiento online para prevenir captación.4. Fortalecer cooperación internacional en monitoreo y desmantelamiento de plataformas ilícitas.5. Establecer canales seguros de denuncia ciudadana contra actividades de reclutamiento o propaganda ilícita.6. Monitorear tendencias discursivas en redes sociales para anticipar campañas de desinformación.7. Integrar a la sociedad civil, academia y medios en estrategias de prevención y comunicación estratégica. |

| | | | |
|---|---|---|---|
| **3. Amenazas mixtas de alto impacto (convergencia técnica y sociopolítica)** | Operaciones complejas coordinadas digitalmente:• Ciberataques a infraestructura crítica combinados con acciones armadas en terreno.• Uso de inteligencia artificial para coordinar redes logísticas, lavado de activos y propaganda simultáneamente.Guerra de información y sabotaje institucional:• Filtración y manipulación de datos estratégicos para desestabilizar gobiernos.• Ataques a procesos electorales combinados con campañas de violencia física.Crimen organizado con doble plataforma (digital-física):• Control territorial reforzado por vigilancia digital y monitoreo de redes sociales locales.• Bloqueo de comunicaciones de seguridad pública antes de acciones criminales.• Uso de criptografía avanzada para coordinar acciones transfronterizas. | Integración metodológica:• Seguridad multidimensional (OEA, 2011) para evaluación global del impacto.• APT + ISO/IEC 27005 para rastreo técnico y gestión de riesgos.• Violencia estructural y cultural (Galtung) para entender motivaciones y contextos.• Conceptualización crítica (Blair Trujillo) para clasificar y priorizar amenazas.• Análisis crítico de redes criminales transnacionales para mapear interconexiones. | Estrategias integrales:1. Crear centros de fusión de inteligencia (CFI) que integren información técnica, operativa y social.2. Desarrollar protocolos de defensa activa que combinen ciberseguridad y operaciones en terreno.3. Establecer mecanismos legales y diplomáticos para respuestas internacionales rápidas.4. Implementar sistemas de redundancia en infraestructura crítica para resistir ataques combinados.5. Desarrollar capacidades ofensivas controladas para desactivar infraestructuras criminales.6. Evaluar continuamente las capacidades institucionales frente a escenarios híbridos complejos.7. Fomentar investigación aplicada en tecnologías de detección anticipada y modelado de escenarios de convergencia criminal. |

Se presenta una comparación entre las amenazas técnicas que operan exclusivamente en el ciberespacio y las amenazas híbridas que, aunque tienen componentes digitales, se articulan con dinámicas sociales, simbólicas o territoriales. En el caso de las amenazas técnicas, como el malware, el ransomware o el lavado de activos con criptomonedas, se aplican marcos como la metodología APT, la norma ISO/IEC 27005 y el componente de seguridad tecnológica del modelo de la OEA, recomendando el fortalecimiento de las capacidades de detección y la gestión de riesgos. Por su parte, las amenazas híbridas como el reclutamiento digital, la propaganda narco o la desinformación en redes sociales requieren una lectura más crítica e interdisciplinaria, que se fundamenta en los aportes de Galtung y Blair Trujillo, así como en la noción de seguridad humana e institucional, promoviendo

acciones como la alfabetización digital, el desarrollo de contranarrativas y la cooperación internacional. Esta comparación evidencia que no todas las amenazas digitales requieren la misma respuesta técnica, sino que exigen enfoques diferenciados que combinen capacidades tecnológicas, análisis estructural y estrategias simbólicas.

## [T1] Conclusiones

Durante el desarrollo de esta investigación, guiada tanto por los objetivos específicos como por la pregunta central, fue posible identificar que las amenazas en el ciberespacio ya sean de tipo técnico o híbrido representan un reto serio y constante para la seguridad nacional. Esta problemática requiere un enfoque que no solo sea multidisciplinario, sino también flexible y en constante evolución. Siguiendo el objetivo de reconocer y clasificar las amenazas técnicas más relevantes, se comprobó que ataques como el malware, ransomware, spear phishing y el uso de criptomonedas con fines ilícitos forman parte de un patrón conocido como Amenazas Persistentes Avanzadas (APT), tal como lo expone Zetter (2014).

ISO/IEC 27005: Norma internacional de gestión de riesgos en seguridad de la información que se traduce en acciones concretas como la construcción de matrices de riesgo, protocolos de respuesta a incidentes, planes de continuidad operativa y sistemas de alerta temprana que priorizan la resiliencia institucional.

Al abordar las amenazas híbridas vinculadas al ciberespacio, se detectó que prácticas como el reclutamiento en línea, la propaganda asociada a economías ilegales y la desinformación en redes sociales no solo comprometen la ciberseguridad, sino que también afectan directamente a la seguridad humana y a la estabilidad de las instituciones. Según las ideas de Galtung (2003) y Blair Trujillo (2009), este tipo de amenazas debilita la cohesión social, genera inestabilidad política y pone en duda la legitimidad institucional. Frente a esto, se vuelve clave impulsar la alfabetización digital, fortalecer la capacidad de respuesta comunitaria y promover la colaboración internacional para hacer frente a campañas de manipulación y guerra psicológica.

En cuanto a la pregunta principal de la investigación relacionada con cómo responder de forma integral a estas amenazas técnicas e híbridas, los hallazgos dejan claro que no basta con aplicar soluciones tecnológicas. Más bien, se necesita una estrategia amplia que incluya varios componentes:

- Tecnología avanzada para detectar y responder a incidentes de manera eficaz.
- Normas claras y actualizadas que adapten los estándares internacionales a la realidad local.

- Participación activa de la ciudadanía y del sector privado como socios claves en la creación de una cultura de ciberseguridad compartida.
- Cooperación internacional para intercambiar información, herramientas y experiencias que ayuden a combatir amenazas globales.

En resumen, el análisis confirma que enfrentar los riesgos del ciberespacio requiere más que acciones reactivas o respuestas fragmentadas. Se necesita un modelo proactivo, integral y resiliente, capaz de anticiparse a los desafíos que presenta el mundo digital. Esto implica, en la práctica, la adopción de tecnología avanzada para detectar y responder a incidentes, la aplicación sistemática de la norma ISO/IEC 27005 en la gestión del riesgo, la implementación de metodologías APT para rastrear amenazas persistentes, y la articulación de políticas públicas que incorporen la seguridad multidimensional de la OEA. A ello se suma la participación ciudadana, la cooperación internacional y la creación de contranarrativas digitales para mitigar la violencia simbólica y estructural que acompaña al narcotráfico en el ciberespacio.

## Referencias

Bada, A., & Nurse, J. R. C. (2020). Developing cybersecurity capacity: A review of research and practical challenges. *Computers & Security, 93*, 101752. https://doi.org/10.1016/j.cose.2020.101752

Baldini, G., & Kounelis, I. (2018). Threat Intelligence and Information Sharing Platforms: Challenges and Opportunities. *Journal of Cybersecurity Technology, 2*(3), 123–140. https://doi.org/10.1080/23742917.2018.1461932

Bayuk, J., Healey, J., Rohmeyer, P., Sachs, M., Schmidt, J., & Weiss, J. (2012). *Cybersecurity Policy Guidebook*. Wiley.

Blair Trujillo, E. (2009). Aproximación teórica al concepto de violencia: avatares de una definición. *Política y Cultura, (32)*, 9-33.

Buzan, B., & Wæver, O. (2003). *Regions and Powers: The Structure of International Security*. Cambridge University Press.

Calderón Concha, P. (2009). Teoría de conflictos de Johan Galtung. *Revista de Paz y Conflictos, 2*, 60-81. https://www.redalyc.org/articulo.oa?id=205016389005

Castells, M. (2012). *Redes de indignación y esperanza: Los movimientos sociales en la era de Internet*. Alianza Editorial.

Cavelty, M. D. (2014). Cyber-security and threat politics: US efforts to secure the information age. Routledge.

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cybersecurity. *Technology Innovation Management Review*, 4(10), 13–21. https://doi.org/10.22215/timreview/835

Dunn Cavelty, M., & Wenger, A. (Eds.). (2022). Cyber Security Politics: Socio-Technological Transformations and Political Fragmentation. Routledge.

Europol. (2022). *Internet Organised Crime Threat Assessment (IOCTA)*. European Union Agency for Law Enforcement Cooperation.

Galtung, J. (2003a). *Trascender y transformar: Una introducción al trabajo de conflictos*. Transcend – Quimera.

Galtung, J. (2003c). *Paz por medios pacíficos. Paz y conflicto, desarrollo y civilización*. Gernika Gogoratuz.

González, F. J., & Rivas, F. A. (2021). Ciberseguridad y crimen organizado transnacional: desafíos para América Latina. Revista de Estudios Estratégicos, 9(18), 45–68.

Interpol. (2023). *Cybercrime Threat Response Report: Latin America 2020–2022*. https://www.interpol.int

Kaspersky Lab. (2022). *Global Cyberthreats Report*. https://www.kaspersky.com

Kello, L. (2017). The Virtual Weapon and International Order. Yale University Press.

Nye, J. S. (2010). Cyber Power. Harvard University, Belfer Center for Science and International Affairs.

Organización de Estados Americanos – OEA. (2011). *Manual de Seguridad Multidimensional*. Secretaría General de la OEA.

Organización de Estados Americanos – OEA. (2020). Ciberseguridad: Riesgos, avances y el camino a seguir en América Latina y el Caribe. https://www.oas.org

ISO/IEC 27005: Norma internacional de gestión de riesgos en seguridad de la información que se traduce en acciones concretas como la construcción de matrices de riesgo, protocolos de respuesta a incidentes, planes de continuidad operativa y sistemas de alerta temprana que priorizan la resiliencia institucional.

Rid, T. (2013). Cyber War Will Not Take Place. Oxford University Press.

Singer, P. W., & Friedman, A. (2014). Cybersecurity and Cyberwar: What Everyone Needs to Know. Oxford University Press.

Tanczer, L. M., Carr, M., & Wright, J. (2018). Gender and cyber security: Research findings and policy recommendations. Global Commission on the Stability of Cyberspace. https://www.gcscc.org

UNODC. (2021). *Darknet and Cryptocurrencies in Drug Markets: Global Trends and Emerging Threats*. United Nations Office on Drugs and Crime.

Zetter, K. (2014). *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*. Crown Publishing Group.

Zohar, A. (2015). Bitcoin: under the hood. *Communications of the ACM, 58*(9), 104–113. https://doi.org/10.1145/2701411