Escandalar Investigativa
Revista Científica

Vol. 2, Núm. (7), Julio – Diciembre (2024)
Depósito Legal: BA2021000019
Articulo Original 26POL3615042026
Área de Conocimiento: Turismo agroecológico, Desarrollo Local y sostenibilidad
Enlace: http://revistas.unellez.edu.ve/index.php/resi

Sistema de Creación Intelectual Vicerrectorado de Producción Agrícola (VPA)

SEGURIDAD CIUDADANA EN LA ERA DE LA INTERCONECTIVIDAD GLOBAL: UN ANÁLISIS SOBRE TENSIONES SOCIOPOLÍTICAS, RIESGOS EMERGENTES Y DESAFÍOS TECNOLÓGICOS ACTUALES.

CITIZEN SECURITY IN THE ERA OF GLOBAL INTERCONNECTIVITY: AN ANALYSIS OF SOCIOPOLITICAL TENSIONS, EMERGING RISKS, AND CURRENT TECHNOLOGICAL CHALLENGES.

Ligia Mercedes Olivares Herrera[1]

Recibido: 01/05/2026 **Aceptado: 11/05/2026**

RESUMEN

Esta investigación analiza la seguridad ciudadana en la era de la interconectividad, enfocándose en cómo las tensiones sociopolíticas y los riesgos emergentes reconfiguran la paz social. El objetivo es evaluar las brechas de seguridad e incertidumbres mediante las normativas que mitiguen crisis y concilien la estabilidad técnica del ciberespacio con la seguridad ciudadanas y la dignidad humana. Ante las amenazas actuales, resulta imperativo identificar los avances y desafíos que definen la seguridad en red, garantizando la integridad de los datos como pilar de la resiliencia en el ciberespacio. Se plantea el uso legítimo de tecnologías avanzadas como Inteligencia Artificial, Big Data y capacidades OSINT al análisis forense. Metodológicamente, se realizó una revisión documental cualitativa, contrastando vacíos

ABSTRACT

This research analyzes citizen security in the age of interconnectivity, focusing on how sociopolitical tensions and emerging risks are reshaping social peace. The objective is to assess security gaps and uncertainties through regulations that mitigate crises and reconcile the technical stability of cyberspace with citizen security and human dignity. Given current threats, it is imperative to identify the advances and challenges that define network security, ensuring data integrity as a cornerstone of resilience in cyberspace. The legitimate use of advanced technologies such as Artificial Intelligence, Big Data, and OSINT capabilities for forensic analysis is being considered. Methodologically, a qualitative document review was conducted, contrasting international legal

Escandalar Investigativa
Revista Cientifica
Vol. 2, Núm. (7), Julio – Diciembre (2024)
Depósito Legal: BA2021000019
Articulo Original 26POL3615042026
Área de Conocimiento: Turismo agroecológico, Desarrollo Local y sostenibilidad
Enlace: http://revistas.unellez.edu.ve/index.php/resi

legales internacionales con el ordenamiento jurídico de Venezuela. Bajo esta premisa, la adopción estratégica de sistemáticas como OSINT y el Big Data, no solo responde a una necesidad técnica de protección, sino a la obligación de construir infraestructuras de defensa analógico que sean auditables, transparentes y alineadas a la seguridad ciudadanas digital. Los resultados revelan estas herramientas es insuficiente si carece de legitimidad social y transparencia institucional, advirtiendo sobre el riesgo de las "cajas negras" algorítmicas. En consecuencia, este estudio concluye que el despliegue transparente, estas infraestructuras se alinea al Plan de la Patria y Artículos 55 y 48 de la Constitución (1999). Robustecer el ecosistema de ciberseguridad nacional surge como la estrategia idónea para neutralizar crisis, recuperar la soberanía digital frente a la creciente sofisticación de los riesgos globales y las tensiones sociopolíticas.

PALABRAS CLAVE: Análisis forense; Ciberespacio; Inteligencia artificial; Ordenamiento jurídico; Seguridad ciudadana.

gaps with the Venezuelan legal framework. Under this premise, the strategic adoption of systems such as OSINT and Big Data not only responds to a technical need for protection, but also to the obligation to build analog defense infrastructures that are auditable, transparent, and aligned with digital citizen security. The results reveal that these tools are insufficient if they lack social legitimacy and institutional transparency, warning of the risk of algorithmic "black boxes." Consequently, this study concludes that the transparent deployment of these infrastructures aligns with the National Development Plan and Articles 55 and 48 of the Constitution (1999). Strengthening the national cybersecurity ecosystem emerges as the ideal strategy to neutralize crises and recover digital sovereignty in the face of the increasing sophistication of global risks and sociopolitical tensions.

KEYWORDS: Forensic analysis; Cyberspace; Artificial intelligence; Legal system; Public safety.

1* **Universidad Nacional Experimental de los Llanos Occidentales Ezequiel Zamora, Barinas, Barinas, Venezuela, correo electrónico:** ligiaolivares123@gmail.com, https://orcid.org/000-0002-45032853.

Escandalar Investigativa
Revista Científica
Vol. 2, Núm. (7), Julio – Diciembre (2024)
Depósito Legal: BA2021000019
Articulo Original 26DER0128032026
Área de Conocimiento: Ciencias Sociales, Jurídicas y Políticas
Enlace: http://revistas.unellez.edu.ve/index.php/resi

Sistema de Creación Intelectual Vicerrectorado de Producción Agrícola (VPA)

1. Introducción

La seguridad ciudadana en la era de la interconectividad ha acelerado la aparición de tensiones sociopolíticas y riesgos emergentes, exigiendo una reconfiguración profunda del contrato social. En este escenario, la labor del Estado ya no puede limitarse a la defensa del territorio tangible debe evolucionar hacia un marco de protección integral, capaz de salvaguardar los sistemas y el flujo de información. Ante la sofisticación de las amenazas, resulta imperativo identificar los avances y desafíos que definen la seguridad en red, garantizando la integridad de los datos como pilar de la resiliencia en el ciberespacio actual.

Bajo este enfoque, Rodríguez (2023) sostiene que el análisis forense es vital para la ciberseguridad venezolana al permitir una respuesta técnica efectiva ante el cibercrimen. Por consiguiente, advierte que la normativa vigente debe ser revisada, ya que la seguridad de los ciudadanos prevista en el artículo 55 de la Constitución (1999), se ve comprometida por fuerzas que operan fuera de los límites del derecho tradicional, lo que exige una rápida adaptación legal ante las nuevas tácticas delictivas. De este modo, el sistema legal constitucional en Venezuela, se ve obligado a evolucionar con la misma celeridad y dinamismo que caracterizan a las nuevas tácticas de la delincuencia informática desafían la efectividad de marcos regulatorios históricos como la Ley Especial contra Delitos Informáticos (2001), la Ley Orgánica de Telecomunicaciones (2000) y la Ley de Infogobierno (2013), los cuales enfrentan un evidente reto de obsolescencia.

Si bien es cierto que, se han promulgado instrumentos recientes el Proyecto de Ley de Inteligencia Artificial, este panorama normativo devela la urgencia de resolver la tensión existente entre la seguridad de los ciudadanos y el Estado en conjunto con las garantías constitucionales. Ante este escenario, surge la necesidad científica de

Escandalar Investigativa
Revista Científica
Vol. 2, Núm. (7), Julio – Diciembre (2024)
Depósito Legal: BA2021000019
Articulo Original 26DER0128032026
Área de Conocimiento: Ciencias Sociales, Jurídicas y Políticas
Enlace: http://revistas.unellez.edu.ve/index.php/resi

precisar ¿de qué manera el diseño de protocolos legales preventivos permite diagnosticar vulnerabilidades sistémicas, en la normativa de ciberseguridad venezolana, asegurando la protección de los derechos fundamentales frente a las nuevas tácticas de la delincuencia informática? A raíz de los protocolos preventivos actúan como mecanismos de auditoría legal que contrastan las conductas delictivas actuales con las leyes vigentes. Al analizar las nuevas tácticas del cibercrimen, se evidencia de forma sistemática que las normativas históricas como la Ley Especial contra Delitos Informáticos (2001) no contemplan dinámicas modernas (como ataques complejos basados en Inteligencia Artificial o suplantaciones de identidad automatizadas).

Este escenario ofrece un diagnóstico preciso de las debilidades regulatorias que demandan corrección prioritaria. Bajo el amparo del Decreto N° 4.975 (Presidencia de la República, 2024), el Consejo Nacional de Ciberseguridad opera como un ente permanente de consulta y asesoría. Debido a que sus metas principales son la vigilancia tecnológica y la seguridad de la infraestructura crítica, el desarrollo de protocolos legales de prevención se convierte en el mecanismo idóneo para consolidar un marco de control institucional eficaz. Al estar basados en principios de proporcionalidad, necesidad y legalidad, establecen límites procedimentales estrictos para evitar que la defensa del ciberespacio derive en la vulneración de la seguridad ciudadana digital (protección de los derechos y libertades en el entorno de red), no depende solo de la vigilancia, sino de superar los vacíos legales históricos mediante marcos normativos robustos y soberanía tecnológica, tal como se proyecta en el Plan de la Patria 2025-2031.

El diseño de estos protocolos estandariza el procedimiento técnico-forense y define exactamente qué datos se pueden recopilar y cómo deben protegerse. Al garantizar que la recolección de evidencia digital se realice bajo el debido proceso, se asegura el

Escandalar Investigativa
Revista Científica
Vol. 2, Núm. (7), Julio – Diciembre (2024)
Depósito Legal: BA2021000019
Articulo Original 26DER0128032026
Área de Conocimiento: Ciencias Sociales, Jurídicas y Políticas
Enlace: http://revistas.unellez.edu.ve/index.php/resi

cumplimiento del Artículo 55 de la Constitución (1999). De este modo, la protección de la integridad y las propiedades de las personas en el entorno digital, no se deja a merced de "fuerzas al margen del derecho tradicional", sino que queda integrada formalmente en el sistema de garantías fundamentales. Por consiguiente, es imperativo que el Estado evalúe las brechas de seguridad y las incertidumbres sociopolíticas mediante el diseño de marcos normativos orientados a la mitigación de crisis.

Esta aproximación regulatoria debe ser capaz de conciliar la estabilidad técnica del ciberespacio con las garantías éticas y los derechos fundamentales de los ciudadanos; un equilibrio que resulta crítico al analizar, bajo esta perspectiva histórica, la evolución de la Inteligencia de Fuentes Abiertas (OSINT) como una metodología originalmente accesible y democrática para la recolección de datos, pero cuyo ecosistema digital contemporáneo atraviesa hoy una transformación radical que amenaza su efectividad. Ante este panorama, la efectividad metodológica no solo responde a las dinámicas del mercado y/o a las políticas de privacidad estatales, sino al surgimiento de barreras técnicas sin precedentes. En la práctica, los investigadores de fuentes abiertas se enfrentan hoy día a un entorno hostil, donde la veracidad de la información pública está en entredicho, debido a la sofisticación de los actores digitales. Ante esta perspectiva, cabe plantearse la siguiente interrogante: ¿Cómo desafían las tecnologías emergentes como los deepfakes, el cierre de APIs y el cifrado masivo la fiabilidad y viabilidad de las investigaciones OSINT en la actualidad? El presente ensayo sostiene que, lejos de quedar obsoleta, la disciplina se encuentra en un punto de inflexión crítico que le exige evolucionar hacia un modelo híbrido de análisis forense digital para garantizar la validez de sus hallazgos en una web cada vez más distorsionada.

2. Fundamentación Teórica

Escandalar Investigativa
Revista Cientifica
Vol. 2, Núm. (7), Julio – Diciembre (2024)
Depósito Legal: BA2021000019
Articulo Original 26DER0128032026
Área de Conocimiento: Ciencias Sociales, Jurídicas y Políticas
Enlace: http://revistas.unellez.edu.ve/index.php/resi

2.1 Desafíos de la seguridad ciudadana en la era de la interconectividad y los riesgos híbridos

En el complejo contexto de la seguridad ciudadana contemporánea, los riesgos han dejado de ser puramente físicos para consolidarse como fenómenos híbridos. La interconexión total entre individuos, instituciones y dispositivos tecnológicos genera tensiones donde el entorno digital impacta directamente en la integridad física y la estabilidad democrática de las naciones. Ante esta transformación, Rodríguez (2023) sostiene que, en un entorno global hiperconectado, emergen riesgos estructurales cuya mayor amenaza radica en el impacto sobre la seguridad financiera. Por consiguiente, este desafío multidimensional trasciende lo técnico y exige una reconfiguración de las políticas de seguridad ciudadana, pues la ausencia de una regulación efectiva del ciberespacio facilita la propagación de conflictos híbridos cuya prevención resulta extremadamente difícil.

Al contrastar el escenario nacional con modelos internacionales, se evidencia que la soberanía tecnológica debe entenderse como la capacidad del Estado para auditar, diseñar y controlar sus propias arquitecturas lógicas. En este sentido, es imperativo sustituir los sistemas cerrados y opacos de proveedores extranjeros por soluciones basadas en código abierto. Esta transición permite desarticular la opacidad algorítmica, garantizando que los protocolos de ciberseguridad actúen bajo principios de transparencia técnica y trazabilidad procedimental. De esta manera, se salvaguardan las garantías éticas y los derechos fundamentales, permitiendo que la tecnología deje de ser una "caja negra" inescrutable y se transforme en un soporte auditable, seguro y confiable para la protección integral de toda la ciudadanía.

En efecto, frente a la porosidad de las fronteras y la sofisticación de las redes delictivas, el modelo de seguridad vertical resulta insuficiente, siendo necesaria una

Escandalar Investigativa
Revista Científica
Vol. 2, Núm. (7), Julio – Diciembre (2024)
Depósito Legal: BA2021000019
Articulo Original 26DER0128032026
Área de Conocimiento: Ciencias Sociales, Jurídicas y Políticas
Enlace: http://revistas.unellez.edu.ve/index.php/resi

estrategia de seguridad en red. Siguiendo a Henao (2025), la capacidad de respuesta institucional ante estos riesgos determinará el futuro de nuestra estabilidad integral. En este ámbito, Venezuela busca cerrar brechas mediante instrumentos como el Código de Ética y el Plan Nacional de Inteligencia Artificial (IA). Al respecto, Cano (2020) afirma que estos pilares son indispensables para una digitalización responsable. Bajo esta visión, la ciberseguridad se consolida como un eje soberano, orientándose prioritariamente a proteger la infraestructura crítica del Estado frente a ataques externos y amenazas complejas.

En último lugar, el mundo enfrenta un creciente fenómeno de cibercrimen que ha democratizado las amenazas, superando las capacidades tradicionales de los organismos de control. Desde la óptica de Bonilla (2025), resulta necesario admitir que, a diferencia de la delincuencia convencional, los delitos digitales como el terrorismo cibernético plantean desafíos que requieren respuestas sistémicas. Bajo esta perspectiva, el entorno venezolano asume la seguridad en red como una necesidad imperativa, generando una tensión inherente entre la búsqueda de independencia tecnológica y la persistente dependencia de infraestructura foránea. Por último, el reto crítico consiste en equilibrar la regulación de contenidos con el principio de democratización al acceso a las tecnologías de información y comunicación.

2.2. Gobernanza digital, analítica forense y el dilema de la autenticidad informativa

En efecto, Vasco (2025) subraya que las naciones aún enfrentan vacíos legales significativos frente al ciberdelito, situación que se replica en Venezuela pese a los mandatos de los artículos 55 y 322 de la CRBV (1999). Al respecto, Barreno (2025) sostiene que el éxito institucional en analítica forense depende de armonizar la eficiencia técnica del Big Data con una legitimidad social que garantice la protección ciudadana, transformando la seguridad en un proceso de construcción colectiva.

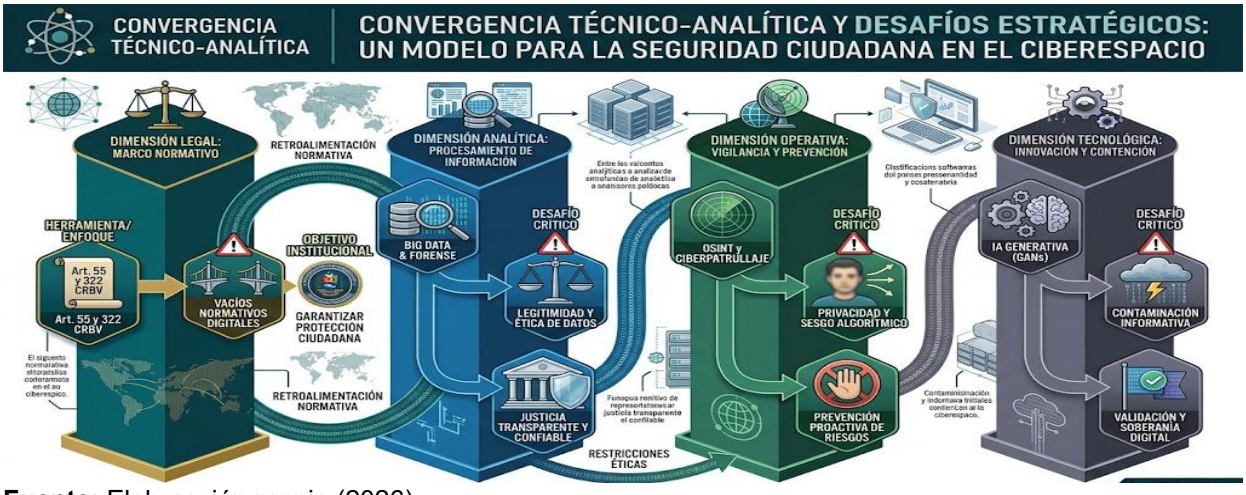
Escandalar Investigativa
Revista Científica
Vol. 2, Núm. (7), Julio – Diciembre (2024)
Depósito Legal: BA2021000019
Articulo Original 26DER0128032026
Área de Conocimiento: Ciencias Sociales, Jurídicas y Políticas
Enlace: http://revistas.unellez.edu.ve/index.php/resi

Simultáneamente, Cano (2022) y Rodríguez et al. (2023) coinciden en que el Estado venezolano transita por un panorama complejo donde, a pesar de las normativas vigentes, persisten desafíos en la confianza técnica. En este sentido, la adopción de sistemas de vigilancia avanzados, inteligencia artificial y ciberpatrullaje mediante OSINT permite anticipar riesgos de forma proactiva, aunque esta práctica suscita controversias estructurales respecto a los límites de la privacidad y el uso ético de los datos masivos.

Por lo tanto, la proliferación de modelos de aprendizaje profundo y archivos sintéticos ha erosionado la base epistemológica tradicional, obligando a los investigadores a integrar auditorías de integridad a nivel de píxel. Por consiguiente, la disciplina OSINT debe evolucionar más allá de las herramientas automáticas de terceros, desarrollando metodologías descentralizadas propias para sortear los muros comerciales impuestos por los grandes consorcios tecnológicos y salvaguardar la veracidad informativa frente a la manipulación digital. Ver Figura 1.

Figura 1.

Convergencia Técnico-Analítica y Desafíos Estratégicos



Fuente: Elaboración propia (2026)

Escandalar Investigativa
Revista Cientifica
Vol. 2, Núm. (7), Julio – Diciembre (2024)
Depósito Legal: BA2021000019
Articulo Original 26DER0128032026
Área de Conocimiento: Ciencias Sociales, Jurídicas y Políticas
Enlace: http://revistas.unellez.edu.ve/index.php/resi

Sistema de Creación Intelectual Vicerrectorado de Producción Agrícola (VPA)

La Figura 1 sintetiza la interacción necesaria entre el marco jurídico, la capacidad operativa y la realidad técnica. Se observa que la dimensión legal actúa como cimiento para la protección, pero requiere de la dimensión analítica y operativa para ser ejecutable en el ciberespacio. La vulnerabilidad central reside en la dimensión tecnológica, donde la irrupción de la IA generativa obliga a las instituciones a transitar desde una vigilancia pasiva hacia una auditoría forense avanzada. En última instancia, la convergencia de estos ejes demuestra que la efectividad de la seguridad ciudadana no emana de la cantidad de datos procesados, sino de la capacidad del Estado para garantizar que cada herramienta técnica cuente con una legitimidad ética robusta frente a la desinformación.

3. Materiales y Métodos

La investigación adopta un enfoque cualitativo, interpretativo y crítico que trasciende la simple cuantificación, posicionando a la ciberseguridad como un complejo entramado de interacciones humanas e institucionales. Mediante un método hermenéutico, el estudio prioriza la calidad del análisis sobre la recolección masiva, asegurando que el uso de herramientas como el Big Data y la analítica forense mantenga una coherencia estricta con los principios democráticos y la legitimidad social del sistema legal vigente.

Asimismo, el procedimiento técnico-metodológico, ejecutado mediante matrices de codificación y triangulación de fuentes, integra la gestión del riesgo como un compromiso global e interconectado. Se utiliza una Matriz de Categorización Técnico-Jurídica que articula el mandato constitucional con capacidades analíticas avanzadas, permitiendo enfrentar desafíos como la opacidad algorítmica y la desinformación. Este diseño busca transformar las amenazas de la hiperconectividad en un equilibrio entre la soberanía tecnológica, la transparencia institucional y la seguridad ciudadana.

4. Resultados

Escandalar Investigativa
Revista Científica
Vol. 2, Núm. (7), Julio – Diciembre (2024)
Depósito Legal: BA2021000019
Articulo Original 26DER0128032026
Área de Conocimiento: Ciencias Sociales, Jurídicas y Políticas
Enlace: http://revistas.unellez.edu.ve/index.php/resi

Sistema de Creación Intelectual Vicerrectorado de Producción Agrícola (VPA)

Este apartado analiza la convergencia entre la innovación informática y los desafíos de seguridad frente a crisis sociopolíticas. La sistematización de hallazgos demuestra que la implementación estratégica de herramientas tecnológicas requiere una reconfiguración de las políticas de protección digital. Se determina que la soberanía tecnológica, fundamentada en un marco ético robusto, constituye el eje determinante para garantizar la estabilidad ciudadana y fortalecer la capacidad de respuesta estatal ante entornos de constante transformación. Ver Tabla 1.

Tabla 1.
Matriz de Categorización Técnico-Jurídica de la Investigación

Categoría Núcleo	Subcategorías Tecnológicas	Definición Operacional	Unidades de Análisis / Herramientas	Indicadores de Aplicación (Art. 55 CRBV)
Garantía Constitucional de la Seguridad Ciudadana en el Ciberespacio *(Art. 55 Constitución-1999)*	Inteligencia de Fuentes Abiertas (OSINT)	Extracción y procesamiento de datos e indicios de acceso público y legal en la web para la identificación temprana de amenazas.	Buscadores especializados (Shodan), SOCMINT (Sherlock, Social-Searcher), rastreo de dominios (Whois).	Prevención proactiva del delito. Alerta temprana de crisis sociopolíticas.
ANALISIS DE BIG DATA		Procesamiento masivo, estructuración y correlación de grandes volúmenes de datos heterogéneos para hallar patrones delictivos.	Algoritmos de raspado (*scraping*), bases de datos correlacionales, modelado de redes complejas (Maltego).	Optimización de la infraestructura técnico-investigativa. Mitigación de riesgos a gran escala.
ANALISIS FORENSE DIGITAL		Auditoría técnica y verificación científica de la integridad de los datos para garantizar su validez legal y evitar la manipulación sintética.	Software de análisis forense multimedia, metadatos, verificación de firmas digitales y detección de *deepfakes*.	Garantías éticas de los administrados. Respeto a los derechos fundamentales y debido proceso.

Escandalar Investigativa
Revista Científica
Vol. 2, Núm. (7), Julio – Diciembre (2024)
Depósito Legal: BA2021000019
Articulo Original 26DER0128032026
Área de Conocimiento: Ciencias Sociales, Jurídicas y Políticas
Enlace: http://revistas.unellez.edu.ve/index.php/resi

Nota: Este instrumento metodológico esquematiza las categorías de análisis crítico que sustentan la investigación. Evidencia que el éxito de la infraestructura investigativa digital no radica en su potencial punitivo, sino en la convergencia ética entre las herramientas de recolección masiva (OSINT/*Big Data*) y las de verificación científica (Analítica Forense), asegurando la protección proactiva frente a las dinámicas estructurales del internet contemporáneo. ***Fuente:*** Elaboración propia (2026) con base de autores.

La reinterpretación del Artículo 55 constitucional posiciona al ciberespacio como un territorio donde el Estado debe garantizar la seguridad ciudadana frente a riesgos emergentes. Esta visión transita hacia un modelo de protección proactiva, integrando metodologías como OSINT y Big Data para procesar información con rigor ético, anticipando amenazas y resguardando libertades. Resulta fundamental que las políticas públicas actuales fortalezcan la ciberseguridad mediante la capacidad institucional de auditar y verificar datos, contrarrestando desafíos como el ciberespionaje o el uso criminal de tecnologías. En consecuencia, la defensa nacional se consolida como una práctica analítica indisoluble, articulando dimensiones técnicas, políticas y jurídicas para asegurar la estabilidad social, equilibrando la respuesta estatal con las garantías ciudadanas en el complejo ecosistema de la comunicación digital. Ver Tabla 2.

Tabla 2.

Garantía Constitucional de la Seguridad Ciudadana en el Ciberespacio

MATRIZ DE CATEGORIA		
NÚCLEO SEGURIDAD CIUDADANA DIGITAL (Art. 55 Constitución-1999)		
Analítica Forense/ Big Data	Legitimidad Social/ Garantías Éticas	Soberanía Tecnológica Plan de la Patria)
Pericia técnica/ Datos masivos	Derechos en la red/ Ciberpatrullaje ético	Autonomía de sistemas/ Protocolos preventivos
CATEGORÍAS EMERGENTES Fase Heurística		
Obsolescencia Legal	Opacidad	Necesidad de Gobernanza

Escandalar Investigativa Revista Científica
Vol. 2, Núm. (7), Julio – Diciembre (2024)
Depósito Legal: BA2021000019
Articulo Original 26DER0128032026
Área de Conocimiento: Ciencias Sociales, Jurídicas y Políticas
Enlace: http://revistas.unellez.edu.ve/index.php/resi

De Larga Data (Leyes)	Cajas Negras	Transfronteriza

Nota: La categoría núcleo Garantía Constitucional de la Seguridad Ciudadana en el Ciberespacio eleva el mandato del Artículo 55 de la Constitución de la República Bolivariana de Venezuela (1999) al rango de garantía fundamental, redefiniendo el ciberespacio como el nuevo territorio digital que el Estado tiene el deber de proteger. **Fuente:** Elaboración propia (2026) con base de autores.

Como consecuencia directa de lo expuesto, garantiza una infraestructura de seguridad ciudadana orientada estrictamente a la mitigación ética de crisis y a la preservación irrestricta de los derechos fundamentales de los administrados, evitando que la recolección masiva de datos devenga en un instrumento de vigilancia o control arbitrario. De acuerdo este abordaje de las amenazas híbridas y la desinformación con las capacidades analíticas de *OSINT* y el *Big Data*, supeditando su éxito técnico a los criterios de validación científica y control de la analítica forense. se fundamenta la matriz de categorización sobre tensiones sociopolíticas y riesgos emergentes en el ciberespacio. Desde este enfoque accede descomponer las variables críticas del entorno virtual, bajo el amparo dogmático del Artículo 55 de la Constitución de la República Bolivariana de Venezuela (1999), sirviendo como mapa analítico para evaluar la confluencia entre las demandas sociales de protección y las capacidades técnicas que ofrecen OSINT, el Big Data y la analítica forense. Ver Tabla 3.

Tabla 3.

Matriz de Categorización sobre Tensiones Sociopolíticas y Riesgos Emergentes en el Ciberespacio.

Categoría Núcleo	Subcategorías Analíticas	Definición Operacional	Unidades de Análisis	Indicadores de Registro
Tensiones Sociopolíticas y Riesgos Emergentes en la Era	Amenazas Híbridas y Desinformación Masiva	Vectores de riesgo basados en la difusión de narrativas falsas o contenido manipulado para	Campañas de bots, medios digitales, foros abiertos, imágenes/video	Patrones de propagación de noticias falsas. Identificación de actores maliciosos. Impacto en la opinión

Escandalar Investigativa
Revista Científica
Vol. 2, Núm. (7), Julio – Diciembre (2024)
Depósito Legal: BA2021000019
Articulo Original 26DER0128032026
Área de Conocimiento: Ciencias Sociales, Jurídicas y Políticas
Enlace: http://revistas.unellez.edu.ve/index.php/resi

Digital (Art. 55 CRBV 1999)		desestabilizar el orden público.	s en zonas de conflicto.	pública.
Inteligencia Operativa de Fuentes Abiertas (OSINT)		Metodología de recolección y análisis de datos públicos para la detección temprana de focos de tensión social o delitos	Redes sociales (SOCMINT), plataformas de mensajería pública, datos de geolocalización	Tiempo de detección de la amenaza. Precisión de las fuentes abiertas. Eficacia de la alerta temprana
Procesamiento Masivo de Datos (Big Data)		Infraestructura técnica para el manejo de volúmenes de datos que permite predecir y mitigar crisis sociopolíticas a gran escala.	Análisis de metadatos, software de detección de deepfakes, auditorías de algoritmos.	Volumen de datos correlacionados. Identificación de patrones predictivos. Velocidad de procesamiento institucional
Validación Científica y Analítica Forense		Protocolos forenses destinados a verificar la autenticidad del dato, garantizando la legitimidad social y el respeto a los DDHH.	Análisis de metadatos, software de detección de deepfakes, auditorías de algoritmos	Tasa de falsos positivos detectados. Preservación del debido proceso digital. Ausencia de vigilancia arbitraria.

Nota: El cuadro sistematiza la transición desde el mandato de prevención proactiva establecido en el Artículo 55 de la Constitución de la República Bolivariana de Venezuela (1999) hacia las dimensiones analíticas del entorno virtual moderno. ***Fuente***: Elaboración propia (2026) con base de autores.

El análisis de las amenazas híbridas y la desinformación Tabla 3 revela que estos vectores actúan hoy como riesgos estructurales con capacidad de fracturar la estabilidad social. Resulta imperativo actualizar la interpretación del Artículo 55 constitucional, expandiendo el deber estatal de protección hacia el ciberespacio, donde se gestan las tensiones sociopolíticas actuales. La gestión efectiva de este desafío exige desarrollar capacidades analíticas avanzadas, como el empleo de metodologías OSINT, permitiendo desmantelar operaciones maliciosas mediante la transparencia y la verdad fáctica. En última instancia, la legitimidad de esta respuesta institucional depende de un equilibrio preciso, garantizando la seguridad pública sin sacrificar los

Escandalar Investigativa
Revista Cientifica
Vol. 2, Núm. (7), Julio – Diciembre (2024)
Depósito Legal: BA2021000019
Articulo Original 26DER0128032026
Área de Conocimiento: Ciencias Sociales, Jurídicas y Políticas
Enlace: http://revistas.unellez.edu.ve/index.php/resi

derechos ciudadanos, evitando así que el control digital derive en censura o limitaciones arbitrarias a la libertad de expresión.

5. Discusión

Al descifrar los procedimientos de categorización, se evidencia que las amenazas actuales operan mediante redes complejas e hiperconectadas. La articulación propuesta conecta la teoría con la praxis al definir subcategorías analíticas para la seguridad digital. Los datos extraídos demuestran que el procesamiento masivo de información heterogénea es la única vía técnica para identificar patrones delictivos latentes y predecir inestabilidades antes de su escalada física. Este hallazgo valida los postulados de Robinson y Vasco (2025), así como las investigaciones de Jahin et al. (2024), quienes sostienen que la seguridad contemporánea depende de la capacidad institucional para transformar volúmenes masivos de información en vectores de prevención estratégica.

Cano y Bernal (2025) señalan que la manipulación algorítmica busca alterar la percepción de la realidad para fracturar la cohesión social mediante redes de bots y *deepfakes*. Esta distorsión de la verdad fáctica se refleja en las tesis de Bernal (2025) sobre las "guerras de quinta generación", donde el flujo informativo en fuentes abiertas constituye el teatro de operaciones para inducir crisis políticas sin confrontación física. Esta realidad empírica colisiona con el marco jurídico interno, observándose una brecha conceptual en el Artículo 55 de la Constitución (1999), diseñado originalmente para el plano fáctico y territorial, lo cual exige redefinir el ciberespacio como una extensión del territorio nacional.

La propagación de narrativas falsas encuentra límites en la Ley Constitucional Contra el Odio (2017) y la Ley Especial Contra los Delitos Informáticos (2001). Quirumbay (2022) advierte sobre la tensión entre la potestad punitiva estatal y la libertad de expresión (Art.

Escandalar Investigativa
Revista Científica
Vol. 2, Núm. (7), Julio – Diciembre (2024)
Depósito Legal: BA2021000019
Articulo Original 26DER0128032026
Área de Conocimiento: Ciencias Sociales, Jurídicas y Políticas
Enlace: http://revistas.unellez.edu.ve/index.php/resi

57, CRBV). No obstante, los resultados demuestran que la vía legítima para la prevención constitucional no es el bloqueo de la red, práctica calificada por Barreno (2025) como un retroceso democrático. La contrastación teórica ratifica, junto a Rodríguez (2023), que la mejor defensa contra amenazas híbridas es el desmantelamiento científico de la desinformación mediante la verificación de datos públicos y auditables.

El procesamiento algorítmico debe mitigar crisis sociopolíticas sin devenir en un control arbitrario que vulnere la seguridad ciudadana digital. La implementación de estas subcategorías choca con tensiones regulatorias, pues la recopilación de datos debe respetar el Artículo 60 de la Constitución (1999) sobre la protección a la vida privada. Taskeen (2024) apunta que el *scraping* masivo camina sobre una delgada línea legal si no se desvincula de datos personales. Así, la legitimidad social exige que el procesamiento se concentre en patrones conductuales colectivos y amenazas verificables, evitando el perfilamiento sistemático e injustificado de los administrados.

Finalmente, este escenario valida a Rodríguez (2023) y Cano (2020) al afirmar que la analítica forense es la única disciplina capaz de devolver la certeza científica a las investigaciones en entornos Web3. La transición hacia una seguridad en red exige auditorías basadas en verificación criptográfica y análisis de cadenas de bloques (blockchain), alineándose con los Artículos 48 y 49 de la Constitución (1999). Como argumenta Aranibar et al. (2022), cualquier indicio que vulnere la privacidad sin orden judicial carece de valor probatorio, confirmando que la analítica forense actúa como un árbitro ético que verifica la autenticidad sin invadir derechos fundamentales.

6. Conclusiones

La seguridad ciudadana en la era de la interconectividad ha evolucionado hacia un desafío híbrido, donde los protocolos de privacidad y el cifrado de las aplicaciones

Escandalar Investigativa
Revista Científica
Vol. 2, Núm. (7), Julio – Diciembre (2024)
Depósito Legal: BA2021000019
Articulo Original 26DER0128032026
Área de Conocimiento: Ciencias Sociales, Jurídicas y Políticas
Enlace: http://revistas.unellez.edu.ve/index.php/resi

modernas neutralizan la recolección pasiva de metadatos tradicionales. Ante esta realidad, el investigador de fuentes abiertas debe trascender la búsqueda de datos visibles para descifrar entornos de información fragmentados, protegidos por sistemas criptográficos que potencian la sofisticación delictiva. Por tanto, el modelo de seguridad vertical y centralizado resulta insuficiente, siendo necesaria una transición hacia una seguridad en red, fundamentada en la corresponsabilidad establecida en el Artículo 55 de la CRBV, como estrategia imperativa para recuperar la soberanía en el ciberespacio.

Esta opacidad digital es una característica estructural de internet que dificulta la trazabilidad de los actores delictivos, obligando a abandonar las técnicas de rastreo lineales. Para superar las barreras del cifrado, los analistas deben integrar herramientas avanzadas que combinen la inteligencia de redes sociales con el análisis de cadenas de bloques y la correlación de identidades digitales a través de múltiples plataformas. La descentralización de la información exige, por tanto, una evolución constante hacia metodologías de investigación que permitan mapear las redes de interacción de manera precisa en un entorno cada vez más complejo y menos predecible.

El estudio confirma que el ciberespacio debe ser tutelado como un nuevo territorio digital bajo la protección del Estado, cuya capacidad de respuesta ante riesgos emergentes depende de una gestión proactiva y coordinada. La efectividad de herramientas como el Big Data y la Inteligencia de Fuentes Abiertas (OSINT) no reside solo en su potencia técnica, sino en su legitimidad social y su estricto apego al ordenamiento jurídico. En el contexto venezolano, esto implica armonizar la capacidad investigativa estatal con las garantías constitucionales de privacidad y el respeto a la inviolabilidad de las comunicaciones, equilibrando la eficiencia técnica con el marco legal vigente.

Escandalar Investigativa
Revista Científica
Vol. 2, Núm. (7), Julio – Diciembre (2024)
Depósito Legal: BA2021000019
Articulo Original 26DER0128032026
Área de Conocimiento: Ciencias Sociales, Jurídicas y Políticas
Enlace: http://revistas.unellez.edu.ve/index.php/resi

En conclusión, la analítica forense digital se posiciona como el árbitro ético y científico indispensable para validar la información sin vulnerar los derechos fundamentales. Solo mediante la implementación de protocolos forenses que auditen la veracidad del dato público, se garantizará que la infraestructura técnica sirva exclusivamente a la protección del pueblo. De esta forma, la respuesta institucional frente al delito no solo alcanzará niveles superiores de eficacia, sino que se mantendrá profundamente justa, ética y humana, asegurando la paz ciudadana en un sistema global interconectado que requiere de soluciones digitales que sean coherentes con la dignidad de las personas.

7. **Referencias**

Aranibar Ramos, E. R., Zanabria Cabrera, L. C., y Daza Ramos, I. H. (2022). Seguridad Ciudadana A Través De Visiones Contrapuestas: Enfoques Desde La Realidad Social en América Latina. *Revista de Filosofía*, *39*(Edición Especial 2), 379-390. https://produccioncientificaluz.org/index.php/filosofia/article/view/39058

Bernal Ontiveros, J. M., Palacios Reyes, M., Zorrilla Briones, F., Rosales Morales, N. R., & Cervantes Cárdenas, S. A. (2025). Ciberseguridad: Métodos de defensa ante ataques de infiltraciones. *RIDE Revista Iberoamericana para la Investigación y el Desarrollo Educativo*, *16*(31). https://www.scielo.org.mx/pdf/ride/v16n31/2007-7467-ride-16-31-e926.pdf

Barreno-Salinas, M. M. (2025). El derecho a la privacidad en la era digital: Desafíos y garantías frente a la vigilancia masiva desde una perspectiva de derechos humanos. *VISUAL REVIEW. International Visual Culture Review*, 17(1), 235-245. https://visualcompublications.es/revVISUAL/article/view/5769/4092.

Escandalar Investigativa
Revista Cientifica
Vol. 2, Núm. (7), Julio – Diciembre (2024)
Depósito Legal: BA2021000019
Articulo Original 26DER0128032026
Área de Conocimiento: Ciencias Sociales, Jurídicas y Políticas
Enlace: http://revistas.unellez.edu.ve/index.php/resi

Bonilla, A. P. H., & Duque, Á. E. A. (2025). Análisis bibliométrico sobre innovación y ciberseguridad: un enfoque estratégico para empresas digitalizadas en Latinoamérica. *Innovare Revista de ciencia y tecnología*, *14*(2), 1-9. https://revistas.unitec.edu/innovare/article/view/563

Constitución de la República Bolivariana de Venezuela. (1999). Gaceta Oficial N° 36.860 (Extraordinaria), 30 de diciembre de 1999. https://www.asambleanacional.gob.ve/storage/documentos/botones/constitucion-nacional-20191205135853.PDF

Cano, J. J. (2020). Seguridad y ciberseguridad 2009-2019. Lecciones aprendidas y retos pendientes. *Revista Sistemas*, (155), 81–94. https://sistemas.acis.org.co/index.php/sistemas/article/view/109

Henao Céspedes V., y Arango Serna, J. C. (2025). *Diseño de una guía metodológica para gestión de incidentes de ciberseguridad* [Trabajo de especialización, Universidad Católica de Manizales]. Repositorio Institucional RI-UCM. https://repositorio.ucm.edu.co/server/api/core/bitstreams/5a002efe-1072-4026-9654-aa65b06897fd/content

Ley Especial Contra los Delitos Informáticos. *Gaceta Oficial de la República Bolivariana de Venezuela*, No. 37.313. https://www.oas.org/juridico/spanish/mesicic3_ven_anexo18.pdf

Ley Constitucional contra el Odio, por la Convivencia Pacífica y la Tolerancia (Reimpresa por error material). *Gaceta Oficial de la República Bolivariana de Venezuela*, No. 41.276. (Original publicada el 8 de noviembre de 2017 en la Gaceta Oficial No. 41.274). https://www.asambleanacional.gob.ve/storage/documentos/leyes/leyconstitucionalcontra-el-odio-por-la-convivencia-pacifica-y-la-tolerancia-20220215163238.pdf

Escandalar Investigativa
Revista Científica
Vol. 2, Núm. (7), Julio – Diciembre (2024)
Depósito Legal: BA2021000019
Articulo Original 26DER0128032026
Área de Conocimiento: Ciencias Sociales, Jurídicas y Políticas
Enlace: http://revistas.unellez.edu.ve/index.php/resi

Ley de Infogobierno. *Gaceta Oficial de la República Bolivariana de Venezuela*, No. 40.274 del 17 de octubre de 2013. https://www.mpppst.gob.ve/mpppstweb/wpcontent/uploads/2015/02/ley_de_infogobierno.pdf.

Ley Orgánica del Plan de la Patria de las 7 Grandes Transformaciones 2025 - 2031. *Gaceta Oficial de la República Bolivariana de Venezuela*, N° 6.907 (Extraordinario), abril 3, 2019 https://mppp.gob.ve/wp-content/uploads/2025/06/GOE-6.907-.pdf.

Ley de Reforma de la Ley Orgánica de Telecomunicaciones, publicada en la Gaceta Oficial de la República Bolivariana de Venezuela N° 6.015 Extraordinario de fecha 28 de diciembre de 2010, reimpresa en la Gaceta Oficial de la República Bolivariana de Venezuela Nº 39.610 de fecha 7 de febrero de 2011. https://pandectasdigital.blogspot.com/2011/02/ley-de-reforma-de-la-ley-organica-de.html

Quirumbay Yagual, D. I., Castillo Yagual, C., & Coronel Suárez, I. (2022). Una revisión del Aprendizaje profundo aplicado a la ciberseguridad. *Revista Científica y Tecnológica UPSE*, *9*(1), 57-65. https://scielo.senescyt.gob.ec/scielo.php?pid=S139076972022000200057&script=sci_arttext

Robinson, R. N. (2025). El fenómeno de la interconectividad y la ciberseguridad: una introducción al objeto del derecho de la ciberseguridad. *Análisis Jurídico-Político*, 7(13), 15-43. https://dialnet.unirioja.es/servlet/articulo?codigo=10565782.

Rodríguez Zambrano, H. M., y Moreno Tamayo, C. H. (2023). Seguridad de la información y ciberseguridad: su importancia para los Estados, empresas y las personas, una revisión sistemática. *Estudios y Perspectivas: Revista Científica y*

Escandalar Investigativa
Revista Científica
Vol. 2, Núm. (7), Julio – Diciembre (2024)
Depósito Legal: BA2021000019
Articulo Original 26DER0128032026
Área de Conocimiento: Ciencias Sociales, Jurídicas y Políticas
Enlace: http://revistas.unellez.edu.ve/index.php/resi

Académica, 4(1) o *Semana de la Salud Ocupacional*. https://colpap.org/wp-content/uploads/2023/12/Articulo-de-revision-sistematica-Ciberseguridad.pdf

Taskeen, Z., y Garai, S. (2024). Emerging trends in cybersecurity: A holistic view of current threats, evaluating solutions, and driving new frontiers. *Journal of Cyber Security and Data Science*, 5(2), 112-128. file:///C:/Users/Ligia/Downloads/10_30953__bhty_v7_302_es.pdf.

Vasco Delgado, J. C., Ruiz Muñoz, G. F., Macas Padilla, B. A., & León Quiñónez, V. H. (2025). Ciberseguridad y protección de datos personales: desafíos y perspectivas. *Revista Científica Gade,* 5(1),675-688. https://revista.redgade.com/index.php/Gade/article/view/642

Conflicto de interés:

Se declara, por parte de la autora, la inexistencia de intereses contrapuestos de ninguna índole en el marco de esta investigación

Fuente de financiamiento:

La autora financio completamente la investigación.

Contribución de autoría:

Ligia Mercedes Olivares Herrera: Gestionó la estrategia, el financiamiento y la revisión crítica. El segundo autor ejecutó la investigación de campo y redacción, mientras el tercero validó resultados mediante análisis estadístico especializado.

Semblanza de la Autor (a)

Ligia Mercedes Olivares Herrera, Abogada. Egresada Universidad UNELLEZ. Especialista en Derecho Procesal Penal. Egresada Universidad Fermín Toro. Línea de investigación perfila en la garantía de los derechos y libertades fundamentales de las personas.

UNELLEZ

Escandalar Investigativa Revista Científica

Vol. 2, Núm. (7), Julio – Diciembre (2024)
Depósito Legal: BA2021000019
Articulo Original 26DER0128032026
Área de Conocimiento: Ciencias Sociales, Jurídicas y Políticas
Enlace: http://revistas.unellez.edu.ve/index.php/resi

Sistema de Creación Intelectual Vicerrectorado de Producción Agrícola (VPA)