N° 1, V. 11 ENERO-JUNIO 2025/ Revista Científica Multidisciplinaria/
ISSN: 2542-3037 https://revistapt.edublogs.org/

CIBERSEGURIDAD COMO EJE ESTRATÉGICO DE LA SEGURIDAD NACIONAL EN VENEZUELA

Darwin Eleazar Martínez Malavé [1,2]

[1]Comisario Jefe del CICPC Jefe de la Coordinación de Desviaciones Policiales del estado Apure [2] darwinmartinezm@gmail.com

Resumen

Este ensayo aborda la ciberseguridad como un pilar estratégico esencial para la defensa y seguridad de Venezuela en un mundo digitalizado. El objetivo es analizar las amenazas cibernéticas actuales, medir la capacidad de respuesta de las instituciones (en especial del Cuerpo de Investigaciones Científicas, Penales y Criminalísticas, CICPC) y proponer un plan de acción integral. Mediante un enfoque cualitativo de análisis de documentos y teorías sobre Protección de Infraestructuras Críticas (PIC) y Estudios Estratégicos, se encuentra que la evolución del cibercrimen, el auge de tecnologías como la inteligencia artificial y el factor humano constituyen las principales debilidades detectadas, lo que obliga a pasar de la criminalística tradicional a la ciberinteligencia. Se concluye que la fortaleza digital de Venezuela se fundamenta en una Estrategia Nacional de Ciberseguridad, la modernización del CICPC, la actualización del marco legal y una fuerte cooperación entre el sector público y privado, ofreciendo así un modelo de gobernanza eficiente para la seguridad digital del país

Palabras clave

Ciberseguridad, Seguridad del Estado, Criminalística Digital, Gobernanza Tecnológica, Infraestructuras Críticas, CICPC.

Recibido: 2025-03- 01 / Revisado: 2025-04-10/ Aceptado: 2025-05-28/ Publicado: 2025-06-30 / Páginas: 293-303

CYBERSECURITY AS A STRATEGIC AXIS OF NATIONAL SECURITY IN VENEZUELA

Darwin Eleazar Martínez Malavé [1,2]

[1]Comisario Jefe del CICPC Jefe de la Coordinación de Desviaciones Policiales del estado Apure [2] darwinmartinezm@gmail.com

Abstract

This essay addresses cybersecurity as an essential strategic pillar for Venezuela's defense and security in a digitalized world. The objective is to analyze current cyber threats, measure the response capacity of institutions (particularly the Scientific, Criminal, and Criminal Investigation Corps, CICPC) and propose a comprehensive action plan. Through a qualitative approach that analyzes documents and theories on Critical Infrastructure Protection (CIP) and Strategic Studies, it is found that the evolution of cybercrime, the rise of technologies such as artificial intelligence, and the human factor constitute the main weaknesses detected, forcing a shift from traditional forensics to cyberintelligence. It concludes that Venezuela's digital strength is based on a National Cybersecurity Strategy, the modernization of the CICPC, the updated legal framework, and strong cooperation between the public and private sectors, thus offering an efficient governance model for the country's digital security.

Keywords

Cybersecurity, National Security, Digital Forensics, Technology Governance, Critical Infrastructure, CICPC.

Recibido: 2025-03- 01 / Revisado: 2025-04-10/ Aceptado: 2025-05-28/ Publicado: 2025-06-30 / Páginas: 293-303

Introducción

La era digital ha transformado por completo la seguridad mundial. Las amenazas ya no son únicamente físicas; ahora existen en un entorno híbrido donde el ciberespacio es un campo de batalla y defensa clave (Kello, 2017). La dependencia de nuestras sociedades de la infraestructura digital, que abarca desde la banca y la energía, hasta el propio gobierno, ha creado una superficie de ataque enorme y difícil de proteger. En este escenario, la ciberseguridad deja de ser un asunto técnico para convertirse en un pilar de la soberanía, la estabilidad económica y la seguridad nacional (Singer y Friedman, 2014).

Las cifras económicas lo confirman, y la percepción de riesgo es compartida a nivel global (Foro Económico Mundial, 2024). Según Morgan (2020, se proyecta que el cibercrimen costará más de 10.5 billones de dólares anuales a nivel mundial para 2025, un costo que se refleja no solo en pérdidas directas sino en la inversión necesaria para mitigar brechas de seguridad (IBM Security, 2023). Este número representa un grave deterioro de la confianza en las instituciones y un peligro para el orden público. Desde una perspectiva teórica, este fenómeno se alinea con los estudios de Protección de Infraestructuras Críticas (PIC), que alertan que la interconexión de los sistemas multiplica el riesgo de que un solo fallo provoque un colapso en cadena (Rinaldi et al., 2001).

Para Venezuela, este panorama global trae consigo tanto desafíos como oportunidades. Proteger sus activos estratégicos y a sus ciudadanos exige que sus organismos de seguridad evolucionen. Por ello, este ensayo busca responder: ¿Qué dimensiones estratégicas se deben fortalecer para construir una arquitectura de ciberseguridad nacional en Venezuela, y cuál es el papel del CICPC en este nuevo esquema? El propósito es analizar las amenazas cibernéticas modernas, evaluar los retos que enfrenta la criminalística digital en el país y proponer un marco de acción basado en cuatro ejes: una estrategia nacional, modernización tecnológica,

cooperación entre instituciones y un marco legal actualizado. Este trabajo es relevante porque puede guiar el diseño de políticas públicas de seguridad y ayudar al CICPC a adaptarse a las nuevas formas del crimen.

Desarrollo argumentativo

Tesis I: la transformación de la amenaza y sus protagonistas

El delito informático ha mutado drásticamente. Lo que antes eran actos de vandalismo digital o simples alardes técnicos, hoy es una industria criminal global, muy organizada y profesional. Amenazas actuales como el *ransomware* ya no buscan solo sabotear, sino que se han convertido en sofisticadas operaciones de extorsión masiva. Este tipo de *malware* no solo secuestra la información de una organización, sino que a menudo la roba para amenazar con publicarla si no se paga el rescate (*double extortion*). El ataque al oleoducto Colonial Pipeline en 2021 es un claro ejemplo; demostró cómo un incidente digital puede causar problemas físicos en la economía real, como escasez de combustible y pánico colectivo. Este suceso confirma las teorías de la PIC sobre la vulnerabilidad que nace de la dependencia entre el ciberespacio y los sistemas físicos esenciales (Easterly, 2023).

Al mismo tiempo, la ingeniería social sigue siendo el método de ataque más común y efectivo, ya que explota directamente la psicología humana. Tácticas como el *phishing* personalizado (*spear phishing*) o el fraude del CEO no dependen de fallos técnicos, sino de manipular la confianza o el sentido de urgencia de una persona. El informe de Verizon (2023) destaca que el 74% de las brechas de seguridad involucran un error humano, lo que demuestra que la tecnología por sí sola no es suficiente. La ciberseguridad es un desafío que combina lo social y lo tecnológico. Como señalan Von Solms y Van Niekerk (2013), una protección real requiere un enfoque que vaya más allá de las barreras técnicas y se centre en la capacitación constante y en crear una cultura de seguridad donde cada persona se sepa parte de la defensa.

El panorama de los atacantes también es más diverso, lo que complica la atribución de los ataques, especialmente cuando se trata de operaciones complejas que involucran múltiples etapas (Clark y Landau, 2010). Además de los cibercriminales que buscan dinero, han surgido actores patrocinados por Estados (*State-Sponsored Actors*). Estos grupos, con recursos casi militares, usan el ciberespacio para el espionaje, el robo de propiedad intelectual o para desestabilizar a otros países, generando un dilema de seguridad entre naciones (Buchanan, 2016; Nye, 2017). A ellos se suman los *hacktivistas*, que usan ataques para promover sus ideas políticas. Esta mezcla de actores y motivaciones —dinero, estrategia geopolítica, protesta— obliga a cuerpos como el CICPC a ir más allá del análisis forense tradicional. Es vital desarrollar una capacidad de ciberinteligencia para entender no solo el "cómo" de un ataque, sino también el "quién" y el "porqué".

Tesis II: el papel del CICPC frente a la criminalística digital

La respuesta del Estado venezolano debe pasar por una profunda adaptación de sus capacidades de investigación penal. El CICPC, como principal órgano de investigación, tiene la tarea de liderar una transición clave: pasar del modelo forense, centrado en la evidencia física, a un paradigma avanzado de criminalística digital. Este cambio es más conceptual que técnico y requiere dominar un conjunto de disciplinas interconectadas:

Análisis forense digital. No se trata solo de recuperar datos. Implica usar métodos científicos rigurosos (como lo establece la norma ISO/IEC 27043:2015 de la International Organization for Standardization, 2015) para adquirir, preservar y analizar evidencia digital de forma que sea válida en un juicio. Los expertos del CICPC se enfrentan a evidencia volátil (como datos en la RAM), a técnicas de antiforense (como el cifrado) y a enormes volúmenes de información. El uso de herramientas como EnCase o FTK es

solo el medio para reconstruir un ciberdelito y atribuir la responsabilidad, manteniendo siempre la cadena de custodia.

Inteligencia de amenazas cibernéticas (CTI). Esta es la evolución de la investigación reactiva a la prevención. En lugar de esperar a que ocurra un ataque, la CTI recolecta y analiza información sobre los atacantes y sus métodos (TTPs). Para el CICPC, esto significa construir un conocimiento que permita anticipar ataques, identificar campañas contra sectores estratégicos y emitir alertas tempranas. Como indican Tounsi y Rais (2018), la CTI permite cambiar la pregunta de "¿Qué pasó?" a "¿Qué podría pasar y quién podría atacarnos?".

Análisis de criptoactivos. El cibercrimen moderno está ligado a las criptomonedas. Monedas como Bitcoin o Monero se usan para lavar dinero o pagar rescates. Es crucial que el CICPC pueda rastrear estas transacciones. Aunque las *blockchains* son públicas, el seudónimo de las billeteras es un reto. Se necesita software especializado (como Chainalysis o Elliptic) que cruce datos para desenmascarar a los criminales, superando herramientas de mezcla (*mixers*) diseñadas para ocultar el rastro de los fondos (Meiklejohn et al., 2013).

Investigación en la red oscura (Dark Web). La *Dark Web* es el mercado de la economía criminal digital. Allí se venden datos robados, *malware* y servicios de ciberataques. Para el CICPC, investigar en este espacio requiere desarrollar perfiles encubiertos, infiltrarse en comunidades criminales y obtener inteligencia en un entorno de alta desconfianza. Es aquí donde a menudo se encuentran las pistas que conectan todas las demás áreas.

Tesis III: hacia una estrategia nacional de ciberseguridad

Una defensa eficaz del ciberespacio no puede ser una suma de acciones aisladas. Requiere una Estrategia Nacional de Ciberseguridad que funcione como una política de Estado. Basada en modelos

internacionales exitosos (como los de la European Union Agency for Cybersecurity [ENISA], o el National Institute of Standards and Technology [NIST], esta estrategia para Venezuela debe apoyarse en los siguientes pilares:

Gobernanza y comando unificado. Lo primero es crear una estructura de mando clara. Es fundamental establecer un Centro Nacional de Respuesta a Incidentes Cibernéticos (CSIRT-Venezuela) que actúe como el comando central para gestionar crisis a gran escala. Este centro debe coordinar la respuesta entre ministerios, agencias de seguridad y operadores de infraestructuras críticas, además de ser el punto de contacto para la cooperación internacional. Como afirman Cavelty y Wenger (2019), institucionalizar la política de ciberseguridad es lo que garantiza una respuesta coherente.

Protección de infraestructuras críticas. Se deben identificar y priorizar las infraestructuras clave del país (energía, agua, finanzas). Sobre ellas, es necesario implementar arquitecturas de seguridad modernas, abandonando los viejos modelos perimetrales. El enfoque de "Confianza Cero" (*Zero Trust*), descrito en la publicación NIST SP 800-207 (National Institute of Standards and Technology, 2020), es el estándar actual. Este modelo no confía en nadie por defecto y verifica cada acceso, lo que reduce drásticamente la superficie de ataque.

Desarrollo de talento humano. La tecnología no sirve de nada sin gente capacitada. La falta de profesionales en ciberseguridad, estimada en más de cuatro millones a nivel global por ISC2 (2024), es una debilidad estratégica. La estrategia nacional debe incluir un programa de formación avanzada para crear expertos en ciberforensia, *ethical hacking* e inteligencia de amenazas, en alianza con universidades y academias policiales.

Marco legal y normativo. La ley suele ir por detrás del ciberdelito. Es urgente actualizar el marco legal para tipificar delitos modernos como

el *ransomware* o el fraude con criptoactivos, con penas proporcionales. Igualmente, es crucial aprobar una Ley de Protección de Datos Personales, inspirada en estándares como el GDPR europeo (Wolford, 2025), para proteger a los ciudadanos y obligar a las empresas a tomarse la seguridad en serio.

Cooperación público-privada e internacional. Nadie puede defender el ciberespacio solo. A nivel nacional, se necesitan alianzas con el sector privado (proveedores de internet, bancos) para intercambiar información de amenazas en tiempo real. A nivel internacional, es vital la cooperación judicial y policial a través de foros como INTERPOL para que las investigaciones tengan consecuencias reales para los criminales, sin importar desde dónde operen.

Conclusiones

Este ensayo ha sostenido que la ciberseguridad es un pilar central para la defensa y seguridad de Venezuela. Se ha demostrado que para construir una arquitectura de ciberseguridad sólida se necesita un enfoque integral que abarque la amenaza, la modernización de instituciones como el CICPC, una estrategia nacional coordinada y leyes adaptadas. En esencia, la resiliencia digital de una nación moderna no se mide solo por su tecnología, sino por su capacidad de crear un ecosistema de seguridad adaptativo. Este sistema debe combinar inteligencia humana, capacidad investigativa, colaboración multisectorial y una gobernanza tecnológica soberana.

Aportes del ensayo

- Teórico: Aplica los marcos de PIC y Estudios Estratégicos al caso venezolano, enriqueciendo la literatura sobre la adaptación de doctrinas de seguridad en América Latina.

- Práctico: Ofrece una hoja de ruta para los líderes políticos, detallando las capacidades que el CICPC necesita y los pilares de una Estrategia Nacional de Ciberseguridad.

Recomendaciones

- Al CICPC: Crear unidades especializadas en ciberforensia, ciberinteligencia y análisis de criptoactivos, y dotarlas de la tecnología y el personal adecuados.
- Al Poder Ejecutivo: Impulsar con urgencia el diseño de la Estrategia Nacional de Ciberseguridad y la creación del CSIRT-Venezuela.
- Al Poder Legislativo: Acelerar la reforma de la Ley Contra los Delitos Informáticos para incluir los nuevos ciberdelitos y debatir una ley de protección de datos personales.

Quedan preguntas por explorar, tales como el impacto de la computación cuántica en la seguridad criptográfica de Venezuela, el desarrollo de modelos para atribuir ciberataques en contextos politizados y el análisis de la cultura de ciberseguridad en la administración pública del país. Lo anterior representa un campo donde ya se están desarrollando nuevos estándares, según el National Institute of Standards and Technology (2022).

Referencias

Buchanan, B. (2016). *The cybersecurity dilemma: Hacking, trust, and fear between nations*. Oxford University Press. https://api.pageplace.de/preview/DT0400.9780190694692_A35478054/preview-9780190694692_A35478054.pdf

Dunn Cavelty, M., & Wenger, A. (2019). Cyber security meets security politics: Complex technology, fragmented politics, and networked science. *Contemporary Security Policy, 41*(1), 5–32. https://www.tandfonline.com/doi/full/10.1080/13523260.2019.1678855#d1e152

Clark, D., & Landau, S. (2010). The problem isn't attribution; it's multi-stage attacks. *Proceedings of the Re-Architecting the Internet Workshop*, (1-6).

https://groups.csail.mit.edu/ana/ANA%20PUBLICATIONS/The_Problem_isnt_Attribution.pdf

Easterly, Jen. (2023. 7 de mayo). *The Attack on Colonial Pipeline: What We've Learned & What We've Done Over the Past Two Years*. Cybersecurity & Infrastructure Security Agency (CISA). CISA blog. https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years

Morgan Steve. (2020, 13 de November). *Cybercrime to cost the World $10.5 trillion annually by 2025*. Cybercrime Magazine. https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

Foro Económico Mundial. (2024). *The global cybersecurity outlook 2024*. https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2024.pdf

ISC2. (2024, 31 de October). *2024 ISC2 Cybersecurity Workforce Study*. https://www.isc2.org/Insights/2024/10/ISC2-2024-Cybersecurity-Workforce-Study

IBM Security. (2023). *Cost of a data breach report 2023*. IBM. https://d110erj175o600.cloudfront.net/wp-content/uploads/2023/07/25111651/Cost-of-a-Data-Breach-Report-2023.pdf

International Organization for Standardization. (2015). *International Standard ISO/IEC 27043:2015 Information technology — Security techniques — Incident investigation principles and processes. (*First edition). ISO/IEC. https://www.amnafzar.net/files/1/ISO%2027000/ISO%20IEC%27043-2015.pdf

Kello, L. (2017). *The virtual weapon and international order*. Yale University Press. https://dokumen.pub/the-virtual-weapon-and-international-order-9780300226294.html

Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoy, D., Voelker, G. M., & Savage, S. (2013). *A fistful of bitcoins: characterizing payments among men with no names.* En Proceedings of the 2013 conference on Internet measurement conference. https://cseweb.ucsd.edu/~smeiklejohn/files/imc13.pdf

National Institute of Standards and Technology. (2020). *NIST Special Publication 800-207: Zero Trust*

Architecture. https://dreamlab.net/wp-content/uploads/2024/11/Arquitectura_de_confianza_cero-NIST.SP_.800-207.pdf

National Institute of Standards and Technology. (2022). *Post-quantum cryptography*. https://www.nist.gov/cybersecurity/what-post-quantum-cryptography

Nye, J. S. (2017). Deterrence and dissuasion in cyberspace. *International Security*, *41*(3), 44–71. https://www.belfercenter.org/sites/default/files/pantheon_files/files/publication/isec_a_00266.pdf

Rinaldi, S. M., Peerenboom, J. P., & Kelly, T. K. (2001). Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Control Systems Magazine*, *21*(6), 11–25. https://www.researchgate.net/publication/3206740_Identifying_understanding_and_analyzing_critical_infrastructure_interdependencies

Singer, P. W., & Friedman, A. (2014). *Cybersecurity and cyberwar: What everyone needs to know*. Oxford University Press. https://api.pageplace.de/preview/DT0400.9780199918102_A23618218/preview-9780199918102_A23618218.pdf

Tounsi, W., & Rais, H. (2018). A survey on technical threat intelligence in the age of sophisticated-attacks. *Computers & Security*, *72*, 212–233. https://es.scribd.com/document/527308196/Tounsi-threat-intelligence

Verizon. (2023). 2023 data breach investigations report (DBIR). https://www.verizon.com/business/resources/reports/2023-data-breach-investigations-report-dbir.pdf

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, *38*, 97–102. https://www.sciencedirect.com/science/article/abs/pii/S0167404813000801

Wolford, Ben. (2025). *¿Qué es el RGPD, la nueva ley de protección de datos de la UE?* GDPR.EU. https://gdpr.eu/what-is-gdpr/