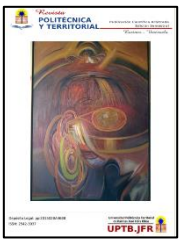
N° 1, V. 11 ENERO-JUNIO 2025/ Revista Científica Multidisciplinaria/
ISSN: 2542-3037 https://revistapt.edublogs.org/



LA SECURITIZACIÓN DE LA CIBERSEGURIDAD EN VENEZUELA: DILEMAS PARA LA SEGURIDAD NACIONAL

Thairys Eliana Carrero Méndez [1,2]

[1] Comisaria CICPC, Jefa Investigaciones Delegación Municipal Chacao, Distrito Capital [2] thairysluciana@gmail.com (http://orcid.org/0009-0009-1794-2663)

Resumen

En Venezuela, la ciberseguridad y la seguridad nacional entablan una relación compleja y tensa, que este ensayo se propone desentrañar mediante el análisis de sus retos, coyunturas favorables y puntos débiles. El objetivo central es investigar de qué manera las dinámicas del ciberespacio han escalado hasta convertirse en prioridades para la seguridad del Estado, y qué repercusiones tiene esta perspectiva sobre la capacidad de resiliencia digital de la nación. La investigación adopta como marco de análisis la Teoría de la Securitización, propia de la Escuela de Copenhague, y se apoya en una revisión de documentos y en el estudio cualitativo de políticas, reportes técnicos y material académico. Lo que se desprende del análisis es una brecha alarmante entre el nivel de sofisticación de las amenazas cibernéticas —que van desde ataques contra infraestructuras hasta operaciones de desinformación— y la limitada capacidad de respuesta del país, una situación agravada por la masiva "fuga de cerebros" y una cultura de ciberseguridad precaria. Con todo, existen oportunidades que emergen de la mano de nuevas tecnologías y de la colaboración internacional. La conclusión principal es que, aunque el proceso de "securitización" es capaz de movilizar recursos valiosos, entraña serios peligros si no va de la mano de estrategias participativas e integrales. El ensayo cierra con un conjunto de recomendaciones orientadas a fortalecer el andamiaje normativo, la formación de talento y la cultura en ciberseguridad, con la meta de consolidar la resiliencia digital como un fundamento de la soberanía nacional.

Palabras clave

Ciberseguridad, Seguridad Nacional, Venezuela, Securitización, Resiliencia Digital, Amenazas Cibernéticas.

Recibido: 2025-02-24 / Revisado: 2025-04-28/ Aceptado: 2025-05-31/ Publicado: 2025-06-30 / Páginas: 395-409

SECURITIZING CYBERSECURITY IN VENEZUELA: DILEMMAS FOR NATIONAL SECURITY

Thairys Eliana Carrero Méndez [1,2]

[1] Comisaria CICPC, Jefa Investigaciones Delegación Municipal Chacao, Distrito Capital [2] thairysluciana@gmail.com (http://orcid.org/0009-0009-1794-2663)

Abstract

In Venezuela, cybersecurity and national security maintain a complex and tense relationship, which this essay aims to unravel by analyzing its challenges, opportunities, and weaknesses. The main objective is to investigate how cyberspace dynamics have escalated to become priorities for state security, and what repercussions this perspective has on the nation's digital resilience capacity. The research adopts the Securitization Theory from the Copenhagen School as its analytical framework and is supported by a documentary review and a qualitative study of policies, technical reports, and academic material. The analysis reveals an alarming gap between the sophistication of cyber threats—ranging from infrastructure attacks to disinformation campaigns—and the country's limited response capacity, a situation worsened by a massive "brain drain" and a precarious cybersecurity culture. Nevertheless, opportunities arise from the adoption of new technologies and international collaboration. The main conclusion is that, while the "securitization" process can mobilize valuable resources, it entails serious dangers if not accompanied by participatory and comprehensive strategies. The essay concludes with a set of recommendations aimed at strengthening the regulatory framework, talent development, and cybersecurity culture, with the goal of consolidating digital resilience as a cornerstone of national sovereignty.

Keywords

Cybersecurity, National Security, Venezuela, Securitization, Digital Resilience, Cyber Threats.

Received: 2025-02-24 / Revised: 2025-04-28 / Accepted: 2025-05-31 / Published: 2025-06-30 / Pages: 395-409

Introducción

Lejos de ser una cuestión puramente técnica, la ciberseguridad se erige hoy como un pilar de la seguridad nacional a escala global (Kshetri, 2021). Para un país como Venezuela, inmerso en un proceso de digitalización irregular y frágil, la administración de los riesgos inherentes al ciberespacio representa un reto estratégico de primer orden. Las vulnerabilidades existentes no se limitan a comprometer sistemas críticos; su alcance es tal que ponen en jaque la estabilidad económica, la gobernabilidad y el propio tejido social.

Es precisamente aquí donde la Teoría de la Securitización, desarrollada por Buzan y su equipo (1998), proporciona una herramienta analítica de gran valor para comprender lo que sucede. Esta teoría postula que ciertos asuntos son discursivamente elevados a la categoría de "amenazas existenciales" por parte de actores con poder —generalmente el Estado— con el fin de legitimar la aplicación de medidas excepcionales. En el caso venezolano, el discurso gubernamental ha interpretado de forma sistemática los fallos tecnológicos, en especial aquellos que impactan los servicios públicos, como parte de una "guerra híbrida" o de "ataques imperialistas" (PRESENCIA ANÁLISIS, 2019; Smilde, 2020). Tal narrativa constituye un evidente acto de securitización, con el que se pretende posicionar al Estado como el único protector válido frente a un adversario tan vago como potente.

Este fenómeno no es un hecho aislado. Reportes de instituciones como la OEA (2020) y de empresas de seguridad como ESET (2023) ya han advertido que América Latina es un blanco cada vez más frecuente de ciberataques de alta complejidad. Si bien la información detallada sobre Venezuela suele ser limitada y poco transparente, los informes de organizaciones nacionales como VE sin Filtro (s.f.) o Espacio Público (2023a) pintan un escenario alarmante. La digitalización acelerada, empujada por la propia crisis y las sanciones internacionales, se da en paralelo a un notable deterioro de la infraestructura tecnológica (Rojas &

Castillo, 2021), lo que genera un terreno fértil para que las vulnerabilidades proliferen.

Así, el propósito de este ensayo es desgranar esa intrincada conexión entre la ciberseguridad y la seguridad del Estado en Venezuela. Se busca analizar de qué modo la percepción de las ciberamenazas, influida por este proceso de securitización, afecta la estabilidad y soberanía del país. Las preguntas que guían este trabajo son: ¿Qué medidas estratégicas se han implementado? ¿De qué forma impacta este enfoque en el ordenamiento jurídico y en la cultura ciudadana de ciberseguridad? Y, como interrogante final, ¿qué enseñanzas podemos obtener para edificar una ciberseguridad que sea, a la vez, más completa y democrática?

Desarrollo

Desafíos y Potencialidades

Bajo el lente de la securitización, los retos de la ciberseguridad dejan de ser meros problemas técnicos para transformarse en amenazas de carácter existencial. Se convierten en vulnerabilidades que el discurso estatal presenta directamente como ataques a la soberanía. Mientras el contexto regional latinoamericano evidencia una escalada en ataques de ransomware y phishing (ESET, 2023), la narrativa oficial en Venezuela tiende a enmarcar los fallos tecnológicos como si fueran actos de agresión externa. Este es un "movimiento securitizador" clásico (Buzan et al., 1998) que se utiliza para legitimar la adopción de medidas extraordinarias, a menudo bajo el argumento de una supuesta "guerra económica" (Álvarez, 2020).

A este panorama se suma la manifiesta vulnerabilidad de la infraestructura crítica nacional, particularmente en los sectores de energía y telecomunicaciones (Sequera & Pardo, 2021). La obsolescencia de los equipos y una crónica falta de inversión en mantenimiento han generado brechas de seguridad que constituyen un peligro latente. El ejemplo más emblemático de esta situación son los masivos apagones de 2019, cuya

causa fue atribuida por la narrativa oficial a un "sabotaje" (Amnesty International, 2019). Este tipo de discurso cumple una doble finalidad: no solo aparta el foco de las verdaderas causas estructurales, sino que también funciona como justificación para intensificar el control por parte del Estado, llegando incluso a la militarización de servicios y áreas consideradas estratégicas (Arconada & Aguilar, 2020).

En el plano jurídico, la estructura normativa del país muestra una fragilidad comparable. La Ley Especial Contra los Delitos Informáticos, promulgada en 2001, fue ciertamente pionera en su momento, pero en la actualidad se muestra claramente superada por la complejidad de amenazas modernas como las Amenazas Persistentes Avanzadas (APTs) o la cripto-extorsión (Carrasquero & Figuera, 2020). Sin embargo, en lugar de avanzar hacia una modernización de la ley basada en el consenso, las propuestas legislativas más recientes, como el controvertido proyecto de "Ley de Ciberespacio", han despertado serias alarmas entre las organizaciones defensoras de los derechos digitales. Estas entidades critican la ambigüedad del texto y advierten sobre su potencial para convertirse en una herramienta de restricción de libertades, en menoscabo de su supuesto fin de proteger a la ciudadanía (Espacio Público, 2023a; Freedom House, 2023).

Para completar este círculo de vulnerabilidades, emergen dos desafíos que se retroalimentan mutuamente. Por una parte, existe un profundo déficit de talento. La migración masiva de profesionales, documentada por el Observatorio de la Diáspora Venezolana (2022), ha supuesto una verdadera sangría de expertos en ciberseguridad, dejando un vacío técnico muy difícil de suplir. Esta carencia, además, nutre la narrativa securitizadora de un Estado que se presenta como indefenso. Por otra parte, la escasa conciencia sobre los riesgos digitales entre la población general (Lugo-Ocando & Hernández-Santaolalla, 2019) la transforma en un objetivo vulnerable a campañas de desinformación y a toda clase de fraudes. Este último fenómeno es, a su vez, enmarcado por

el Estado como una amenaza a la estabilidad nacional, lo que le ha servido de justificación para reforzar el control sobre el flujo de información, un hecho que queda patente en la controversial Ley Constitucional contra el Odio (República Bolivariana de Venezuela, 2017).

Oportunidades Estratégicas

A pesar de este complejo escenario, el panorama no es enteramente desolador. Existe la posibilidad de abordar la ciberseguridad no como un arma en un conflicto, sino como un desafío técnico y de desarrollo. Este enfoque, que se alinea con un proceso de "desecuritización" selectiva (Wæver, 1995), permitiría abrir el camino hacia soluciones de carácter más colaborativo y sostenible. Adoptar esta perspectiva significa trascender la retórica del enfrentamiento para centrar los esfuerzos en el fortalecimiento de las capacidades genuinas del país.

Las tecnologías emergentes representan una vía de oportunidad significativa. Si bien es cierto que la experiencia con la criptomoneda Petro estuvo plagada de opacidad y generó desconfianza (Zambrano, 2020), la tecnología que la sustenta, como es el blockchain, alberga un potencial considerable para mejorar la transparencia y la seguridad de los registros públicos. De manera similar, la Inteligencia Artificial, que ya se ha consolidado como un pilar de la ciberdefensa a nivel mundial (OCDE, 2021), podría ser aprovechada para la detección proactiva de amenazas. Sin embargo, su implementación exige, como condición indispensable, un debate público amplio sobre su gobernanza y sus implicaciones éticas, a fin de prevenir que derive en un instrumento de vigilancia masiva.

Quizás la oportunidad más crítica se encuentra en la formación de capital humano. Instituciones universitarias como la UCV y la USB continúan siendo baluartes académicos sólidos. Una política de Estado firme, liderada por el Ministerio de Ciencia y Tecnología (MPPCT, s.f.), tiene el potencial de articular programas de especialización, sistemas de certificación y alianzas estratégicas con el sector privado. El objetivo sería doble: por un lado, retener al talento existente y, por otro, reciclar las

habilidades de otros profesionales. Esta no sería un gasto, sino una inversión estratégica fundamental para, al menos parcialmente, frenar y eventualmente revertir la fuga de cerebros que tanto ha afectado al país.

La cooperación internacional, siempre que se aborde con pragmatismo y se logre despolitizar, representa otra avenida de gran valor. A pesar de las tensiones que puedan existir en otras áreas, la colaboración técnica con entidades como la Unión Internacional de Telecomunicaciones (UIT) o el Foro Global de Expertise en Ciberseguridad (GFCE) puede facilitar el acceso a mejores prácticas y a sistemas de alerta temprana. Finalmente, se presenta una oportunidad nítida en el ámbito regulatorio: desarrollar un marco legal que, en vez de adoptar un enfoque restrictivo, se armonice con los estándares internacionales de derechos digitales, como los que promueve la CIDH (2017). Un paso de esta naturaleza sería fundamental para reconstruir la confianza, tanto en el plano doméstico como en el internacional.

Fortalezas y resiliencia.

Aun con el complejo panorama descrito, Venezuela no se encuentra en un punto de partida nulo. El país cuenta con cimientos tanto institucionales como humanos que, si se logran consolidar, podrían servir de base para una estrategia de ciberseguridad mucho más sólida.

El principal baluarte a nivel institucional radica en la existencia de la Superintendencia de Servicios de Certificación Electrónica (SUSCERTE) y de su brazo ejecutor, el VeCERT (s.f.). Más allá de su mera existencia formal, esta entidad acumula un acervo de experiencia de más de una década en la gestión de incidentes y en la difusión de alertas. Dicha memoria institucional, con todos sus aciertos y desaciertos, constituye un activo de incalculable valor y representa el núcleo lógico a partir del cual se podría construir una arquitectura de ciberdefensa nacional de mayor envergadura.

En lo que respecta al capital humano, y aunque el impacto de la diáspora ha sido ciertamente devastador, resultaría un desacierto

subestimar a la comunidad técnica que aún reside en Venezuela. Egresados de reconocidas casas de estudio como la UCV (s.f.) y la USB (s.f.), complementados por una gran cantidad de autodidactas y miembros activos de comunidades de software libre y ciberseguridad, han forjado una impresionante capacidad de adaptación y de innovación, a menudo con medios muy restringidos. Este talento, aunque disperso, constituye una fuerza latente que, si se logra convocar y equipar adecuadamente, podría ser clave para la resiliencia del país.

Por último, existe una fortaleza de naturaleza intangible pero de importancia crítica: la experiencia adquirida en la adversidad. La exposición continua a crisis y a fallos en los servicios básicos ha obligado a segmentos del sector técnico y de la sociedad civil a idear soluciones creativas y planes de contingencia. Esta cultura de "resolver" los problemas en contextos de elevada incertidumbre, si bien es producto de la necesidad, puede transformarse en una ventaja competitiva al momento de concebir sistemas que no solo sean seguros, sino también resilientes y con la capacidad de funcionar incluso en condiciones adversas.

Amenazas y peligros latentes

Los peligros que enfrenta el entorno digital en Venezuela son tangibles y de múltiples caras, trascendiendo con creces la simple retórica política. La inteligencia global de firmas de prestigio como Microsoft (2023) y Check Point Research (2023) corrobora la presencia activa en América Latina de actores hostiles, entre los que se incluyen grupos de Amenazas Persistentes Avanzadas (APTs), con frecuencia auspiciados por Estados. Sus metas son diversas y abarcan desde el sabotaje de infraestructuras vitales hasta el espionaje industrial y la sustracción de información estratégica de organismos públicos y empresas privadas (CSIS, 2022).

De especial virulencia es la amenaza que representa la desinformación. Las operaciones de influencia, documentadas de manera exhaustiva por observatorios especializados como ProBox (s.f.), Cazadores de Fake News (s.f.) y el DFRLab del Atlantic Council, persiguen

un fin mucho más profundo que la mera propagación de noticias falsas. Su verdadero objetivo es agudizar la polarización social, minar la confianza en las instituciones y los medios de comunicación, y en última instancia, manipular el debate público. Este tipo de amenaza se aprovecha de una cultura mediática deficiente y se erige como un arma estratégica capaz de desestabilizar el país desde su interior.

No obstante, los peligros no son exclusivamente externos; las amenazas internas continúan constituyendo un factor de riesgo de primer orden. El error humano —desde un empleado que cae en una trampa de phishing hasta un servidor mal configurado— es universalmente reconocido como una de las principales brechas de seguridad en los ciberataques (SANS Institute, 2023). En un entorno como el venezolano, caracterizado por una alta rotación de personal y una formación continua insuficiente, este riesgo se ve notablemente amplificado. A ello se le añade el peligro de las amenazas internas malintencionadas, es decir, empleados con acceso privilegiado que deliberadamente sabotean sistemas o filtran datos sensibles; un riesgo que a menudo queda eclipsado por la espectacularidad de los ataques externos.

Conclusiones

En esencia, la ciberseguridad en Venezuela se manifiesta como un terreno de disputa política, en el cual las urgencias técnicas de protección quedan supeditadas a los imperativos de la seguridad nacional. Al aplicar la lente de la Teoría de la Securitización, se hace evidente la tendencia del Estado a enmarcar las amenazas del ciberespacio —ya sean fallos técnicos o campañas de desinformación— como un peligro existencial para la soberanía. Este "acto de habla" con el que se securitiza un tema (Buzan et al., 1998) no solo tiene como fin la movilización de recursos, sino también la legitimación de medidas que pueden resultar en un control más férreo sobre el ecosistema digital (Espacio Público, 2023a).

El presente análisis permite inferir que un proceso de securitización que no vaya de la mano de un robustecimiento simultáneo de las

capacidades nacionales, de la institucionalidad democrática y de una cultura de ciberseguridad inclusiva, se arriesga a ser contraproducente. Tal enfoque podría fácilmente derivar en un círculo vicioso de mayor control estatal que, sin embargo, no se traduzca en una resiliencia digital real y efectiva (DeNardis & Hackl, 2015). Ante este panorama, las fortalezas ya identificadas —como la existencia de SUSCERTE y el potencial del mundo académico—, sumadas a las oportunidades que ofrece la cooperación técnica, señalan la existencia de vías alternativas.

En definitiva, al estudiar el caso venezolano a través de este marco, se comprueba que la securitización es mucho más que una simple respuesta a una amenaza: se constituye como un instrumento de gobernanza cuyas implicaciones se extienden profundamente al ámbito de los derechos humanos (Human Rights Watch, 2023) y a la naturaleza misma de la seguridad que dice defender.

Recomendaciones estratégicas

Más que un simple listado, las siguientes recomendaciones se estructuran como un conjunto de ejes estratégicos que se refuerzan mutuamente.

• Eje Normativo e Institucional: Resulta imperativo promover una legislación sobre ciberseguridad que sea contemporánea, que se fundamente en estándares internacionales (UIT, s.f.; IGF, s.f.) y que logre un equilibrio justo entre la seguridad, la protección de los datos personales y la libertad de expresión, en línea con las directrices de la CIDH (2017). Esta reforma legal debe ir acompañada de la conformación de una instancia nacional de carácter multisectorial —que aglutine al Estado, el sector privado, la academia y la sociedad civil— para asegurar una coordinación coherente de los esfuerzos.

• Eje de Capital Humano y Cultura: Se debe otorgar máxima prioridad a la inversión estratégica en talento, lo que implica robustecer los programas universitarios existentes (Consejo Nacional de Universidades, s.f.) y diseñar incentivos claros para la retención de profesionales. De

forma paralela, es crucial desplegar programas nacionales de amplio alcance para la alfabetización digital y mediática, en alianza con organizaciones de la sociedad civil (Medianálisis, s.f.; IPYS Venezuela, 2023), con el fin de forjar una ciudadanía más crítica y resiliente.

• Eje Tecnológico y de Cooperación: Es fundamental priorizar la inversión destinada a la modernización y aseguramiento de las infraestructuras críticas, adoptando para ello estándares de reconocimiento global (como la norma ISO 27001). Esta prioridad incluye la exploración de tecnologías como la Inteligencia Artificial (OCDE, 2021) dentro de marcos éticos bien definidos, así como la búsqueda activa de una cooperación técnica despojada de sesgos políticos a través de foros globales como FIRST.org.

Nuevas líneas de indagación

Esta investigación abre la puerta a interrogantes fundamentales que ameritan ser explorados en futuros trabajos. Sería pertinente, por ejemplo, evaluar con rigurosidad el impacto socioeconómico real que han tenido los ciberataques en sectores clave de la economía venezolana. Resultaría de gran valor emprender un análisis comparado sobre las estrategias de securitización de la ciberseguridad en naciones con contextos políticos análogos. Asimismo, investigar la efectividad real de las campañas de alfabetización digital como contrapeso a la desinformación, o analizar el papel potencial que la diáspora podría desempeñar en la transferencia de conocimiento, representan rutas de estudio muy prometedoras.

Referencias

Álvarez, R. (2020). La "guerra económica" contra Venezuela: narrativas y discursos. *Revista Venezolana de Economía y Ciencias Sociales*, 26(1), 135–155.

Amnesty International. (2019). *Venezuela: Hunger, punishment and fear: The ongoing human rights crisis in Venezuela*. Amnesty International Ltd.

Arconada, S., & Aguilar, S. (2020). Militarización y seguridad ciudadana en Venezuela. *URVIO, Revista Latinoamericana de Estudios de Seguridad*, (27), 75–92. https://doi.org/10.17141/urvio.27.2020.4226

Atlantic Council Digital Forensic Research Lab (DFRLab). (s.f.). *Investigations*. https://www.atlanticcouncil.org/programs/digital-forensic-research-lab

Buzan, B., Wæver, O., & de Wilde, J. (1998). *Security: A new framework for analysis*. Lynne Rienner Publishers.

Carrasquero, J. V., & Figuera, A. J. (2020). Delitos informáticos en Venezuela: Un análisis desde la perspectiva de la Ley Especial. *Telos: Revista de Estudios Interdisciplinarios en Ciencias Sociales*, 22(2), 335–351.

Cazadores de Fake News. (s.f.). *Investigaciones*. https://www.cazadoresdefakenews.info

Center for Strategic and International Studies (CSIS). (2022). *Significant Cyber Incidents*. https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

Check Point Research. (2023). *Cyber Attack Trends: 2023 Mid-Year Report*. Check Point Software Technologies Ltd.

Comisión Interamericana de Derechos Humanos (CIDH). (2017). *Estándares para una internet libre, abierta e incluyente*. OEA/Ser.L/V/II. CIDH/RELE/INF. 24/17.

Consejo Nacional de Universidades. (s.f.). *Programas Académicos*. https://loeu.opsu.gob.ve

DeNardis, L., & Hackl, A. M. (2015). Internet governance by social media platforms. *Telecommunications Policy*, 39(9), 761–770. https://doi.org/10.1016/j.telpol.2015.04.003

ESET. (2023). *Panorama de amenazas en Latinoamérica 2023*. ESET Latinoamérica. https://www.welivesecurity.com/es/informes/eset-security-report-2023-seguridad-empresas-america-latina/

Espacio Público. (2023a). *Informe anual 2022: El cerco a la crítica*. https://espaciopublico.ong/informe-2022-situacion-del-derecho-a-la-libertad-de-expresion-e-informacion-en-venezuela/

Foro de Gobernanza de Internet (IGF). (s.f.). *Best Practice Forums*. https://www.intgovforum.org/en/content/best-practice-forums-bpfs

Foro Global de Expertise en Ciberseguridad (GFCE). (s.f.). *About Us*. https://thegfce.org

Freedom House. (2023). *Freedom on the Net 2023: Venezuela*. https://freedomhouse.org/country/venezuela/freedom-net/2023

Human Rights Watch. (2023). *World Report 2023: Venezuela*. https://www.hrw.org/world-report/2023/country-chapters/venezuela

IPYS Venezuela. (2023). *Educación digital*. https://ipysvenezuela.org/2023/05/10/reporte-derechos-digitales-2023/

Kshetri, N. (2021). Cybersecurity and international relations. *Journal of Global Information Technology Management*, 24(3), 173–177. https://doi.org/10.1080/1097198X.2021.1934240

Lugo-Ocando, J., & Hernández-Santaolalla, V. (2019). Media literacy and public service media in Latin America: Challenges for citizens' empowerment. *Comunicar*, 27(60), 19–28. https://doi.org/10.3916/C60-2019-02

Medianálisis. (s.f.). *Formación*. https://www.medianalisis.org/formacion/

Microsoft. (2023). *Microsoft Digital Defense Report 2023*. https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report

Ministerio del Poder Popular para Ciencia y Tecnología (MPPCT). (s.f.). *Programas*. https://mincyt.gob.ve

Observatorio de la Diáspora Venezolana. (2022). *Informe anual sobre la diáspora venezolana*. https://www.elimpulso.com/2022/10/05/observatorio-de-la-diaspora-venezolana-68-de-la-poblacion-piensa-emigrar-5oct/

Organización de los Estados Americanos (OEA). (2020). *Informe de amenazas de ciberseguridad en las Américas 2020*. https://www.oas.org/es/sms/cicte/docs/Informe-Ciberseguridad-2020.pdf

Organización para la Cooperación y el Desarrollo Económicos (OCDE). (2021). *Artificial intelligence and the future of cybersecurity*. OECD Publishing. https://doi.org/10.1787/4f4c8a78-en

Presencia Análisis. (2019, 11 de marzo). El ciberataque: nueva fase de la guerra contra Venezuela. *Aporrea.org*. https://www.aporrea.org/tecno/a275617.html

ProBox. (s.f.). *Investigaciones*. https://proboxve.org/investigaciones

República Bolivariana de Venezuela. (2017, 8 de noviembre). *Ley Constitucional contra el Odio, por la Convivencia Pacífica y la Tolerancia*. Gaceta Oficial No. 41.274.

Rojas, A., & Castillo, O. (2021). Crisis de los servicios públicos en Venezuela: Una aproximación desde la perspectiva de los derechos humanos. *Revista de Ciencias Sociales (Ve)*, 27(Especial 4), 22–38. https://doi.org/10.31876/rcs.v27i.36506

SANS Institute. (2023). *SANS Security Awareness Report*. https://www.sans.org/blog/2023-security-awareness-report/

Sequera, J., & Pardo, M. (2021). La crisis eléctrica venezolana: entre el colapso infraestructural, la emergencia humanitaria compleja y la ecología política del extractivismo. *Ecología Política*, (61), 59–66.

Smilde, D. (2020, 23 de enero). Is Venezuela a victim of hybrid warfare? *Washington Office on Latin America (WOLA)*. https://www.wola.org/analysis/venezuela-victim-hybrid-warfare/

Superintendencia de Servicios de Certificación Electrónica (SUSCERTE). (s.f.). *VeCERT*. https://vencert.suscerte.gob.ve/about-us

Unión Internacional de Telecomunicaciones (UIT). (s.f.). *Cybersecurity*. https://www.itu.int/en/ITU-D/Cybersecurity/Pages/default.aspx

Universidad Central de Venezuela (UCV). (s.f.). *Facultad de Ingeniería*. https://www.ing.ucv.ve

Universidad Simón Bolívar (USB). (s.f.). *Departamento de Computación y Tecnología de la Información*. https://www.ci.usb.ve

VE sin Filtro. (s.f.). *Reportes*. https://vesinfiltro.org/res/files/reporte-2022-2023.pdf

Wæver, O. (1995). Securitization and desecuritization. En R. D. Lipschutz (Ed.), *On security* (pp. 46–86). Columbia University Press.

Zambrano, E. (2020, 6 de febrero). El petro a dos años de su lanzamiento: entre el desconocimiento y la desconfianza. *Prodavinci*. https://prodavinci.com/el-petro-a-dos-anos-de-su-lanzamiento-entre-el-desconocimiento-y-la-desconfianza/