SECURITIZAR LA INFRAESTRUCTURA CRÍTICA: UNA REVISIÓN DE LAS ESTRATEGIAS NACIONALES DE CIBERSEGURIDAD EN ESTADOS UNIDOS (2003-2023)

María Fernanda Artunduaga Ospina
Director de Tesis: Andrés Arturo Peña Galindo
Cotutor: Felipe Higuera Angulo
Fecha de presentación: 11 de abril de 2025

Programa de Ciencia Política
Facultad de Ciencias Jurídicas y Políticas
Universidad El Bosque

Resumen:

En un contexto de creciente interconexión digital, el ciberespacio se ha consolidado como un ámbito estratégico para la seguridad nacional, particularmente en Estados Unidos, donde la protección de la infraestructura crítica nacional (ICN) ha sido una prioridad. Desde 2003, las Estrategias Nacionales de Ciberseguridad (ENC) han representado el principal instrumento de formulación para responder a las amenazas emergentes en el entorno digital. Esta investigación analiza las ENC entre 2003 y 2023, con el propósito de identificar cómo han sido configuradas en relación con la protección de la ICN en función de las amenazas y desafíos en el ciberespacio. Para ello, se adopta la teoría de la securitización de Barry Buzan, Ole Wæver y Jaap de Wilde (1998) como marco analítico, lo que permitirá establecer categorías conceptuales que expliquen la influencia de las amenazas cibernéticas en la formulación de las ENC. La metodología empleada se basa en el análisis de contenido de documentos oficiales a través del software *NVivo*, mediante un sistema de categorización que facilitará la identificación de patrones y transformaciones en las ENC a lo largo del período estudiado.

Abstract:

In a context of increasing digital interconnection, cyberspace has become a strategic domain for national security, particularly in the United States, where the protection of national critical infrastructure (NCI) has been a priority. Since 2003, the National Cybersecurity Strategies (NCS) have served as the primary policy instrument for addressing emerging threats in the digital environment. This research analyzes the NCS between 2003 and 2023, aiming to identify how they have been structured concerning NCI protection in response to threats and challenges in cyberspace. To achieve this, the study adopts the securitization theory of Barry Buzan, Ole Wæver, and Jaap de Wilde (1998) as an analytical framework, allowing for the establishment of conceptual categories that explain the influence of cyber threats on the formulation of NCS. The methodology is based on content analysis of official documents using NVivo software, applying a categorization system that will facilitate the identification of patterns and transformations in the NCS over the studied period.

Palabras clave:

Ciberseguridad, Infraestructura crítica, Estrategias nacionales de ciberseguridad, Securitización, Ciberespacio.

Keywords:

Cybersecurity, Critical Infrastructure, National Cybersecurity Strategies, Securitization, Cyberspace.

Tabla de contenidos

I. Introducción **5**
II. Marco teórico **9**
III. Metodología **16**
IV. Ciberseguridad en clave securitizadora: una mirada a las ENC de 2003 a 2023 **19**
V. Conclusiones **33**
VI. Bibliografía **34**

I. Introducción

En el siglo XXI, se ha observado un constante aumento en el uso del ciberespacio a nivel mundial. Según la Unión Internacional de Telecomunicaciones (UIT), para el 2023, "aproximadamente el 67% de la población global, es decir, 5.400 millones de personas, estaban conectadas a Internet, lo que representa un crecimiento del 4,7% respecto al año anterior" (UIT, 2024). Este aumento ha intensificado las amenazas a la seguridad nacional, particularmente a la infraestructura crítica de ciberpotencias como Estados Unidos. De acuerdo con la Oficina de la Responsabilidad del Gobierno de Estados Unidos (2024), los sistemas informáticos federales y la infraestructura crítica del país se enfrentan a un riesgo creciente. Las agencias federales han informado más de 30.000 incidentes de seguridad informática desde el año 2022. En esta investigación, se tomará a Estados Unidos como referente analítico, dado que el Índice Nacional de Ciberpoder (NCPI, por sus siglas en inglés), elaborado por la Universidad de Harvard, sostiene que Estados Unidos cuenta con el mayor poder cibernético a nivel mundial, definido como "el despliegue efectivo de ciber-capacidades por parte de un estado para lograr objetivos nacionales" (Voo, Hemani & Cassidy, 2022, p. 7). Esto se refleja en una capacidad instalada superior en materia de protección y gestión de su infraestructura crítica.

Esta situación subraya la necesidad de Estados Unidos de proteger su **infraestructura crítica nacional** (ICN, de ahora en adelante) con el fin de salvaguardar su seguridad nacional, al considerar que dicha infraestructura abarca los "activos, sistemas y redes que proporcionan funciones necesarias para nuestro modo de vida. [...], cualquier amenaza a estos sectores podría tener consecuencias potencialmente debilitadoras para la seguridad nacional, la economía y la salud o la seguridad pública" (CISA, 2024a). Ejemplos de esta infraestructura incluyen los bancos, las bases de datos de seguridad social y las plantas de energía nuclear. Por ello, en respuesta a la creciente vulnerabilidad en el ciberespacio, Estados Unidos ha venido implementado desde el año 2003 las **estrategias nacionales de ciberseguridad** (ENC, de ahora en adelante). Estas estrategias han sido concebidas como un marco integral destinado a proteger la integridad del país. Al asegurar la protección de la ICN y mitigar las amenazas cibernéticas que se presentan en el ciberespacio, dado que:

> Proporciona orientación a los departamentos y agencias del gobierno federal que desempeñan funciones en la seguridad del ciberespacio. También identifica los pasos

> que pueden dar los gobiernos estatales y locales, las empresas y organizaciones privadas y los estadounidenses a título individual para mejorar nuestra ciberseguridad colectiva. La Estrategia destaca el papel del compromiso público-privado. (...) La dinámica del ciberespacio exigirá ajustes y modificaciones de la Estrategia a lo largo del tiempo. (The White House, 2003, p. 8)

Por consiguiente, las estrategias tienen como propósito prevenir y reducir las vulnerabilidades del país en el ciberespacio mediante una acción conjunta y coordinada de todos los actores involucrados. De igual manera, estas estrategias se actualizan periódicamente para abordar las amenazas y desafíos emergentes en el ciberespacio. Desde 2003 hasta 2023, Estados Unidos ha emitido cuatro (4) ENC, cada una reflejando las prioridades y desafíos para la protección de la ICN del país en el ciberespacio.

La primera estrategia, la "*Estrategia Nacional para la Seguridad del Ciberespacio*", fue publicada en 2003 durante la administración de George W. Bush (2001-2009). Esta estrategia fue pionera en establecer un marco de acción para proteger la ICN del país frente a las amenazas cibernéticas, al sentar las bases de la cooperación público-privada en materia de ciberseguridad. Posteriormente, en 2011, bajo el gobierno de Barack Obama (2009-2017), se presentó la "*Estrategia Nacional de Ciberseguridad*", la cual subrayó la importancia de la cooperación internacional en la defensa de la ICN y la promoción de un ciberespacio seguro y abierto. En 2018, durante la administración de Donald Trump (2017-2021), se emitió la "*Estrategia Nacional de Ciberseguridad*", que recalcó la necesidad de fortalecer la resiliencia de la ICN a través de la innovación tecnológica y la inversión en capacidades defensivas. Finalmente, en 2023, bajo la administración de Joe Biden (2021-2024), se publicó una nueva "*Estrategia Nacional de Ciberseguridad*", que se enfoca en la protección integral de la ICN mediante una mayor regulación, cooperación con el sector privado y alianzas internacionales.

No obstante, es crucial tener en cuenta que la protección de la ICN requiere entender su carácter contingente. Estas infraestructuras son complejas e interdependientes, “lo que significa que dependen unas de otras y, al mismo tiempo, están en continuo cambio y se adaptan a numerosos cambios en la economía, la legislación, la tecnología, etc.” (Leroy & Zolotaryova, 2023, p. 166). En consecuencia, el impacto de un ciberataque podría amplificarse, dado que “el fallo de un sistema de infraestructura crítica puede afectar en cascada a otro y causar daños aún mayores” (Leroy & Zolotaryova, 2023, p. 166). Por lo

tanto, las ENC deben ser dinámicas y capaces de adaptarse a un entorno de amenazas en constante evolución. En ese sentido, el presente artículo busca responder a la siguiente pregunta de investigación: **¿de qué manera se han configurado las estrategias nacionales de ciberseguridad en Estados Unidos como respuesta a las amenazas y desafíos emergentes en el ciberespacio, en relación con la infraestructura crítica, durante el período comprendido entre 2003 a 2023?**

De acuerdo con lo anterior, el objetivo principal de esta investigación es: **analizar** la configuración de las estrategias nacionales de ciberseguridad en Estados Unidos durante el periodo 2003-2023, enfocadas en la protección de la infraestructura crítica en respuesta a las amenazas y desafíos emergentes en el ciberespacio. Para desarrollar dicho objetivo general, se plantean los siguientes tres objetivos específicos: primero, **identificar**, desde el marco teórico de la securitización, las categorías conceptuales utilizadas para representar la infraestructura crítica en las estrategias nacionales de ciberseguridad de Estados Unidos durante el periodo 2003-2023. Segundo, **describir**, la transformación de la concepción de la infraestructura crítica en las estrategias nacionales de ciberseguridad de los Estados Unidos, mediante un análisis de contenido para destacar los principales cambios implementados entre 2003 y 2023. Por último, **interpretar** las configuraciones que han tenido las estrategias nacionales de ciberseguridad en los Estados Unidos, a partir de las amenazas y desafíos contra la infraestructura crítica provenientes del ciberespacio en el periodo 2003-2023.

En este orden de ideas, la estructura interna del artículo se dividirá en cuatro secciones: en la primera sección, se ofrecerá un marco teórico en el que se establecerán cuatro categorías conceptuales, amparadas en la *teoría de la securitización,* para entender la concepción de infraestructura crítica reflejada en las estrategias nacionales de ciberseguridad entre 2003-2023. En la segunda sección, se analizarán las estrategias nacionales de seguridad publicadas por el gobierno de Estados Unidos para estudiar la concepción de la infraestructura crítica, a partir de la metodología cualitativa de *análisis de contenido*. En la tercera sección, se interpretarán los resultados, a partir de las categorías conceptuales operativizadas y las evidencias extraídas en la primera y segunda sección, respectivamente; de este modo, se espera responder a la pregunta inicial de investigación. Por último, se finalizará con el apartado de conclusiones.

Esta investigación contribuye a la ciencia política desde una perspectiva internacionalista, al abordar la ciberseguridad como un tema emergente y fundamental dentro de la subdisciplina de los estudios de seguridad. Al enfocarse en las ENC de Estados Unidos, el artículo no solo enriquece el debate académico sobre el tema (Azmi et al., 2018; Craig et al., 2022; Granata, 2019), sino que también ofrece un análisis detallado de las medidas implementadas por el país en las últimas dos décadas para proteger su ICN frente a las amenazas y desafíos cibernéticos en constante evolución. Asimismo, a través de una visión crítica, se examina la capacidad de estas estrategias para adaptarse a la naturaleza dinámica del ciberespacio, al analizar sus configuraciones mediante la identificación y caracterización de las principales amenazas y desafíos. Por consiguiente, los resultados de esta investigación proporcionan herramientas teóricas para comprender cómo las políticas de ciberseguridad de los gobiernos de Estados Unidos han respondido a las cambiantes amenazas y desafíos dirigidos contra su ICN.

La teoría de la securitización, propuesta por Barry Buzan, Ole Wæver y Jaap de Wilde (1998), es el marco que permite ilustrar cómo se configuran las amenazas y desafíos percibidos en las ENC. Esta teoría sostiene que, a través del discurso, se puede construir y designar una amenaza que justifique la implementación de medidas, como las estrategias de seguridad, para erradicarla. Según los autores (1998), el significado de un concepto radica en su uso práctico más que en una definición analítica o filosófica, y se manifiesta en cómo se utiliza implícitamente en ciertos contextos. En el ámbito de la seguridad nacional, identificar un fenómeno como una amenaza es un proceso de construcción social, donde el problema se presenta como una cuestión de seguridad que requiere una solución. La seguridad es, por tanto, una práctica autorreferencial, ya que es el propio proceso de securitización lo que convierte un asunto en una amenaza, no necesariamente por la existencia de un peligro real, sino porque se presenta como tal (Buzan et al., 1998). La relevancia de esta teoría reside en su capacidad para explicar cómo la securitización es un proceso discursivo que designa amenazas o desafíos sobre la infraestructura crítica, los cuales son institucionalizados en Estados Unidos a través de las ENC, con el fin de proteger dicha infraestructura frente a las amenazas y desafíos observados según las circunstancias del momento.

Asimismo, es fundamental abordar los conceptos de ciberespacio, ciberseguridad e ICN. El ciberespacio “no solo incluye internet, sino que abarca infraestructuras físicas de información

y telecomunicaciones, códigos y protocolos entre máquinas, así como regulaciones e ideas normativas, constituyendo una red interdependiente que entrelaza sistemas digitales y físicos" (Vila y Marcelo, 2019). Ante la creciente interconexión, y las amenazas emergentes en este espacio, surge la ciberseguridad como "el arte de proteger redes, dispositivos y datos de accesos no autorizados o usos delictivos y la práctica de garantizar la confidencialidad, integridad y disponibilidad de la información" (CISA, 2021). Esta protección se extiende a la ICN, que comprende "activos y sistemas esenciales para el funcionamiento del estado, la sociedad y la economía, como agencias federales, salud, energía, transporte y tecnología" (The White House, citado en Sam, 2023).

Por otra parte, a partir de la propuesta metodológica de Hernandez et al. (2014), esta investigación se enmarca en un enfoque cualitativo, con un alcance descriptivo y un diseño de *análisis de contenido*. El enfoque cualitativo permitirá profundizar en los discursos dentro de las estrategias emitidas por el gobierno de Estados Unidos a través de la identificación, categorización y sistematización de la información contenida en documentos clave, tales como las ENC. El alcance descriptivo se justifica en la necesidad de detallar y contextualizar cómo se han formulado y adoptado estas estrategias para enfrentar las amenazas y desafíos del ciberespacio a lo largo de las dos últimas décadas. De igual forma, el diseño metodológico será el de un *análisis de contenido*, centrado en la identificación de patrones discursivos y configuraciones de amenazas y desafíos en los documentos gubernamentales seleccionados. Para llevar a cabo este análisis, se empleará el software *NVivo*, que permitirá organizar, codificar y analizar los datos de manera eficiente, para facilitar la identificación de categorías conceptuales y relaciones entre las variables establecidas.

II. Marco teórico

Para comenzar, esta investigación se sitúa en el ámbito de la ciberseguridad dentro de los estudios de seguridad en las Relaciones Internacionales, particularmente en los Estudios Críticos de Seguridad desarrollados por la Escuela de Copenhague. En este contexto, se aborda la **teoría de la securitización**, propuesta por los académicos Barry Buzan, Ole Wæver y Jaap de Wilde en su obra, *Security: A New Framework for Analysis* (1998). En este libro los autores buscan establecer un nuevo marco global para los estudios de seguridad, al ampliar la definición tradicional de seguridad, que tiende a limitarse a la supervivencia en términos político-militares. Según los autores, "en términos generales, equiparan la seguridad con las

cuestiones militares y el uso de la fuerza" (Buzan et al., 1998, p. 1). Frente a esta visión, los autores proponen una concepción multidimensional de la seguridad que contemple amenazas en sectores como el económico, medioambiental y social. Afirman que "[nuestra solución consiste en] ampliar la agenda de seguridad, manteniéndola abierta a muchos tipos diferentes de amenazas. [...] Explorando las amenazas a los objetos de referencia y la securitización de esas amenazas, que son tanto militares como no militares" (Buzan et al., 1998, p. 4).

No obstante, para mantener la coherencia intelectual en torno a lo que se puede considerar seguridad en las Relaciones Internacionales, su significado debe ser más específico que cualquier amenaza o problema que surja en un determinado sector. En este caso, la seguridad se entiende como una construcción discursiva, en la cual "algo se designa como un asunto de seguridad internacional porque se puede argumentar que ese asunto es más importante que otros y debería tener prioridad absoluta" (Buzan et al., 1998, p. 24). Bajo esta premisa, no existe un fenómeno social llamado intrínsecamente seguridad, sino que esta se construye y se designa discursivamente como tal, cuando los actores involucrados asumen la presencia de algo determinado como una amenaza, que requiere una respuesta mediante el despliegue de medidas para contrarrestarla. Según los autores,

> [e]l significado de un concepto reside en su uso y no es algo que podamos definir analítica o filosóficamente según lo que sería 'mejor'. El significado no reside en lo que la gente piensa conscientemente que significa el concepto, sino en cómo lo utilizan implícitamente de unas maneras y no de otras. (Buzan et al., 1998, p. 24)

En otras palabras, la securitización es una emisión realizativa que, en términos de teorías de actos de habla, entiende que la enunciación y proferencia del concepto instituye su propia realidad institucional. En lo que respecta a la seguridad nacional de Estados Unidos, cuando se identifica un fenómeno como una amenaza o desafío para la ciberseguridad del país, especialmente con relación con la ICN, se lleva a cabo un proceso de construcción social intersubjetivo. En este proceso, el fenómeno se presenta como una amenaza que exige una solución; lo importante aquí es la construcción discursiva del problema y su establecimiento como un asunto de ciberseguridad. Por ello, se señala que "[l]a 'seguridad' es, por tanto, una práctica autorreferencial, porque es en esta práctica que la cuestión se convierte en una

cuestión de seguridad, no necesariamente porque exista una amenaza existencial real, sino porque la cuestión se presenta como tal amenaza" (Buzan et al., 1998, p. 25).

En consecuencia, la securitización sigue una estructura retórica específica basada en la noción de "supervivencia" y la "prioridad de acción", bajo la premisa de que "si el problema no se maneja ahora, será demasiado tarde y no existiremos para remediar nuestro fracaso" (Buzan et al., 1998, p. 26). Por esta razón, cuando se estudia un caso de securitización, no se trata de evaluar amenazas "que "realmente" pongan en peligro algún objeto que deba ser defendido o asegurado. Más bien, el enfoque está en comprender los procesos de construcción de una comprensión compartida acerca de qué se debe considerar y responder colectivamente como una amenaza" (Buzan et al., 1998, p. 26).

Por esta razón, con el fin de comprender los actos de habla en los procesos de securitización —particularmente aquellos articulados en las ENC de Estados Unidos para enfrentar las amenazas y desafíos en el ciberespacio en relación con las ICN entre 2003 y 2023— se establecerán cuatro categorías conceptuales: (i) **tipos de infraestructura crítica,** (ii) **actores,** (iii) **contexto y** (iv) **amenazas.** Estas se fundamentan en las unidades clave del análisis de la seguridad propuestas por Buzan, Wæver y de Wilde, complementadas con aportes provenientes de la literatura académica especializada en ciberseguridad. El objetivo de estas categorías es abordar de manera integral los factores determinantes en la construcción discursiva de las amenazas y desafíos identificados en cada periodo, al considerar el contexto político en el que emergieron, los actores que impulsaron dichos discursos y, en particular, la identificación de las ICN como elementos centrales en las estrategias de protección.

En primer lugar, la categoría de ***tipos de infraestructura crítica* (*types of critical infrastructure*)** constituye una unidad analítica central en los procesos de securitización, al fungir como el ***objeto de referencia***, definido como "aquello que se considera existencialmente amenazado y que tiene un derecho legítimo a sobrevivir" (Buzan et al., 1998, p. 36). En el contexto de las ENC, este ***objeto de referencia*** está representado por las ICN, cuya función es esencial para el sostenimiento de los servicios vitales de un país. Dado su carácter estratégico, cualquier vulnerabilidad en estas infraestructuras se percibe como una amenaza existencial, lo que justifica la implementación de medidas de protección como las ENC. Según CISA:

> [h]ay 16 sectores de infraestructuras críticas cuyos activos, sistemas y redes, ya sean físicos o virtuales, se consideran tan vitales para Estados Unidos que su incapacidad o destrucción tendría un efecto debilitador sobre la seguridad, la seguridad económica nacional, la salud o la seguridad pública nacional, o cualquier combinación de éstas. (CISA, 2024b).

Estos sectores, detallados en la Tabla 1, se entienden como subcategorías de análisis, ya que cada uno desempeña un papel estratégico e interdependiente dentro del funcionamiento general del Estado. En este sentido, la categoría de ***tipos de infraestructura crítica*** resulta indispensable para identificar los sectores cuya protección es prioritaria a fin de garantizar la continuidad de los servicios esenciales y la estabilidad nacional. Cada uno representa un sistema altamente interconectado, cuya afectación podría desencadenar efectos en cascada con consecuencias significativas para la seguridad y la economía del país (CISA, 2024b).

En segundo lugar, los **actores (*actors*)** desempeñan un papel fundamental en la teoría de la securitización, al constituir una de las unidades analíticas propuestas por los autores para comprender los actos de habla que conforman los procesos de securitización. Son quienes identifican y consolidan una amenaza mediante el uso del discurso. Esta categoría se divide en dos (2) tipos: por un lado, (i) los ***actores securitizadores***, definidos como aquellos que "securitizan cuestiones declarando algo —el objeto referente— como una amenaza existencial" (Buzan et al., 1998, p. 36). Se trata de actores con la capacidad de construir discursivamente una amenaza, valiéndose de su legitimidad y posición de poder; entre ellos se encuentran las élites políticas y las burocracias. Por otro lado, (ii) los ***actores funcionales***, aquellos que, sin ser el objeto referente ni quienes reclaman seguridad en nombre del objeto referente, ejercen una influencia significativa en las decisiones relativas al ámbito de la seguridad (Buzan et al., 1998). Su intervención puede materializarse a través de la provisión de información técnica, la implementación de políticas o la presión indirecta sobre las agendas públicas. Así, esta categoría analítica permite identificar tanto a los actores securitizadores como a los funcionales involucrados en la construcción de las ENC y su contribución a la protección de las ICN.

En tercer lugar, la categoría de ***contexto* (*context*)** se refiere al "conjunto de circunstancias y factores que influyen en la interpretación de un mensaje, incluyendo elementos extralingüísticos como el lugar, el tiempo, las relaciones sociales y las intenciones comunicativas" (Van Dijk, 2008). Este marco espacio-temporal constituye la base para los

procesos de securitización, ya que determina la percepción de las amenazas por parte de los actores y orienta la forma en que estas son construidas discursivamente. Desde la teoría de la securitización, el contexto es un elemento clave para comprender la interacción entre actores y la construcción social de los riesgos, en tanto permite articular respuestas estratégicas orientadas a su contención (Buzan et al., 1998). Esta categoría se subdivide en tres (3) subcategorías:

(i) ***La interdependencia entre el ciberespacio y las Infraestructuras Críticas Nacionales*** **(*Interdependence of Cyberspace and NCIs*)**, que analiza cómo las ENC han construido históricamente la relación entre las ICN y el ciberespacio. Esta interdependencia abarca múltiples dimensiones —sociales, políticas y digitales—, lo que exige una comprensión integral de sus implicaciones (Shannon Prier et al., 2023). Su relevancia radica en examinar cómo las ENC conceptualizan la necesidad de proteger estas interconexiones para prevenir los riesgos inherentes a las ICN.

(ii) ***El impacto de las amenazas y vulnerabilidades del ciberespacio*** **(*Impact of Cyberspace Threats and Vulnerabilities*)**, permite identificar los efectos concretos de dichas amenazas sobre las instituciones gubernamentales y la cotidianidad de los estadounidenses, "los ciberataques se han extendido por una amplia área, desde la vida cotidiana hasta las instituciones gubernamentales, la economía hasta el comercio y los bancos hasta hospitales" (Aslan, 2023, p. 19). Esta subcategoría visibiliza la necesidad de diseñar estrategias de mitigación, como las ENC, frente a escenarios de riesgo cada vez más complejos y transversales.

(iii) ***La normatividad en materia de ciberseguridad nacional en Estados Unidos*** **(*U.S. National Cybersecurity Regulations*)**, examina los marcos legales y regulatorios citados en las ENC y orientados a la protección de las ICN frente a las amenazas cibernéticas. Esta subcategoría determina si se incluyen lineamientos técnicos y regulaciones como el Marco de Ciberseguridad del NIST, HIPAA, GLBA, FISMA, CISA, CCPA y los DoD (Oluomachi et al., 2024).

Estas subcategorías permiten analizar las dimensiones estructurales, técnicas y normativas que configuran el contexto de las ENC, en tanto han influido en su formulación, así como en la identificación de las ICN como objetos de referencia que requieren protección frente a amenazas emergentes. Este enfoque responde al núcleo de los estudios de seguridad

propuesto por la teoría de la securitización, que sitúa "la supervivencia de las unidades y principios colectivos —la política de la amenaza existencial— como el núcleo definitorio de los estudios de seguridad, proporcionando una base para aplicar el análisis de seguridad a una variedad de sectores sin perder la calidad esencial del concepto" (Buzan et al., 1998, p. 27).

Por último, la categoría de ***amenazas* (*threats*)** constituye uno de los conceptos centrales de la teoría de la securitización, al representar el elemento que justifica el acto de securitizar. La Escuela de Copenhague retoma en parte la concepción schmittiana de la política, basada en la lógica disociativa del antagonismo. En términos de Carl Schmitt, "la distinción política específica, aquella a la que pueden reducirse todas las acciones y motivos políticos, es la distinción de amigo y enemigo" (Schmitt, 1932, p. 2). Esta lógica implica una diferenciación radical entre quienes comparten intereses y valores comunes (los *amigos*) y quienes son percibidos como una amenaza (los *enemigos*), a quienes se atribuyen relaciones de hostilidad o indiferencia.

En el contexto de la teoría de la securitización, la amenaza no se define por su existencia, sino por su construcción discursiva como un enemigo existencial. Esta construcción permite justificar decisiones políticas, como la formulación de ENC orientadas a la protección de las ICN. Así, lo que instaura una amenaza como tal es su identificación y tratamiento en el discurso político como un riesgo que exige medidas. "La amenaza puede ser real o percibida como tal por parte de las autoridades, los medios de comunicación y la opinión pública, quienes comparten la percepción de su potencial de daño extraordinario que requiere medidas políticas urgentes" (Demurtas, 2019, p. 170).

En consecuencia, la determinación de si un fenómeno debe ser securitizado —por ejemplo, mediante las ENC— depende de su potencial para poner en riesgo las ICN. Además, como advierten Buzan et al. (1998), "una amenaza sólo puede entenderse en relación con el carácter particular del objeto de referencia en cuestión. No estamos tratando aquí con un estándar universal basado en algún sentido de lo que amenaza la vida humana individual" (p. 22). Por tanto, la naturaleza de la amenaza varía según el sector y el objeto que se busca proteger, en este caso, la ICN. Por ende, en este caso, para esta categoría se subdivide en tres (3) subcategorías:

(i) *La naturaleza y los tipos de ciberamenazas* (*Nature and Types of Cyber Threats*), que analiza cómo las ENC clasifican las amenazas cibernéticas en función de su origen

y tipología, tales como *ransomware*, ataques de *phishing*, denegación de servicio distribuida (*DDoS*) o amenazas móviles (Aslan, 2023, p. 16). Esta clasificación constituye la base discursiva de las ENC sobre la cual se justifica la necesidad de proteger las ICN.

(ii) ***Las vulnerabilidades en las ICN y en el ciberespacio*** **(*Vulnerabilities in the NCI and Cyberspace*)**, se refiere a las debilidades estructurales o técnicas que comprometen a las ICN. Como señala Aslan (2023), "una vulnerabilidad es una falla dentro de un producto o sistema que potencialmente puede permitir que un atacante socave la confidencialidad, integridad o disponibilidad de ese producto o sistema" (p. 19). Estas vulnerabilidades intensifican el impacto potencial de las ciberamenazas y posicionan a las ICN como objetivos estratégicos.

(iii) ***Los actores maliciosos y sus motivaciones*** **(*Malicious Actors and Their Motivations*)**, aborda a los agentes responsables de las ciberamenazas, al destacar que "los humanos, no las computadoras, crean las amenazas informáticas [...] cualquier persona que utilice una computadora conectada a Internet debe ser consciente de las amenazas que representan los hackers y depredadores" (Ömer Aslan, 2023, p. 17). En el marco de la teoría de la securitización, estos actores se instauran discursivamente como enemigos, conforme a la distinción schmittiana entre amigo-enemigo, lo que refuerza la necesidad de adoptar medidas como las ENC.

Estas subcategorías son fundamentales porque permiten delimitar el marco discursivo y operativo para la construcción de las amenazas y de los enemigos existenciales. En este sentido, como afirman Buzan et al. (1998), la amenaza no puede analizarse aisladamente del objeto de referencia; por tanto, la identificación de estas es clave para comprender la adaptación de las ENC para la protección de las ICN.

Finalmente, las categorías y subcategorías propuestas (ver Tabla 1) son esenciales para este análisis, ya que constituyen la base conceptual y discursiva para comprender los elementos que justificaron la necesidad de intervención estatal en la protección de las ICN frente a las amenazas y riesgos del ciberespacio. En este marco, la teoría de la securitización ofrece un enfoque analítico para interpretar cómo se construyen discursivamente las amenazas, cómo los actores validan dichas construcciones y de qué manera se diseñan políticas específicas —como las ENC— para mitigar estos riesgos. En conjunto, estas categorías garantizan un

abordaje integral y multidimensional que permite explicar los desafíos que cada administración ha enfrentado en materia de ciberseguridad.

Tabla 1. ***Categorías y Subcategorías para el Análisis de Contenido***

Categorías	Subcategorías
Tipos de Infraestructura Crítica (*Types of Critical Infraestructure*)	1. Sector químico *(Chemical Sector)*. 2. Sector de las instalaciones comerciales *(Commercial Facilities Sector)*. 3. Sector de las comunicaciones *(Communications Sector)*. 4. Sector manufacturero crítico *(Critical Manufacturing Sector)*. 5. Sector Presas *(Dams Sector)*. 6. Sector de la base industrial de defensa *(Defense Industrial Base Sector)*. 7. Servicios de emergencia *(Emergency Services Sector)*. 8. Sector energético *(Energy Sector)*. 9. Sector de Servicios Financieros *(Financial Services Sector)*. 10. Sector Agroalimentario *(Food and Agriculture Sector)*. 11. Servicios e instalaciones gubernamentales *(Government Services and Facilities Sector)*. 12. Sector Sanitario y Salud Pública *(Healthcare and Public Health Sector)*. 13. Sector de las Tecnologías de la Información *(Information Technology Sector)*. 14. Reactores nucleares, materiales y residuos *(Nuclear Reactors, Materials, and Waste Sector)*. 15. Sector de Sistemas de Transporte *(Transportation Systems Sector)*. 16. Sector del agua y las aguas residuales *(Water and Wastewater Sector)*.
Actores (*Actors*)	1. Actores securitizadores *(Securitising actors)*. 2. Actores funcionales *(Functional actors)*.
Contexto (*Context*)	1. Interdependencia del ciberespacio y las ICN (*Interdependence of cyberspace and NCIs*). 2. Impacto de las amenazas y las vulnerabilidades del ciberespacio (*Impact of cyberspace threats and vulnerabilities*). 3. Normatividad de la ciberseguridad nacional de los Estados Unidos (*U.S. National cybersecurity regulations*).
Amenazas (*Threats*)	1. Naturaleza y tipos de ciberamenazas *(Nature and types of cyber threats)*. 2. Vulnerabilidades en la ICN y el ciberespacio *(Vulnerabilities in the NCI and cyberspace)*. 3. Actores maliciosos y sus motivaciones *(Malicious actors and their motivations)*.

Fuente: Elaboración propia con base en la información obtenida de CISA (2024) y *Security: A New Framework for Analysis* (1998) de Barry Buzan, Ole Wæver y Jaap de Wilde.

III. Metodología

Para continuar, la metodología de esta investigación se enmarca en un enfoque cualitativo, con un alcance descriptivo y un diseño basado en el *análisis de contenido*. El método

cualitativo se centra en describir, comprender e interpretar fenómenos sociales desde una perspectiva interpretativa y subjetiva, a partir del uso de una lógica inductiva (Hernández et al., 2014). Este enfoque busca "establecer las relaciones y significados asociados a su objeto de estudio" (Sánchez, 2005, p. 4). De este modo, las investigaciones cualitativas se orientan hacia la comprensión del "por qué" y el "cómo" de los fenómenos. Además, esta investigación tiene un alcance descriptivo, ya que “busca especificar las propiedades, las características y los perfiles de personas, grupos, comunidades, procesos, objetos o cualquier otro fenómeno que se someta a un análisis” (Hernández, 2024, p. 28). En este sentido, los enfoques cualitativos y descriptivos son adecuados para la presente investigación, ya que permite un análisis profundo e interpretativo de los discursos presentes en las ENC. A través de la categorización y sistematización de estas estrategias, es posible identificar y comprender, desde sus respectivos contextos, cómo han surgido las configuraciones adoptadas para la protección de la ICN, en respuesta a las amenazas y desafíos del ciberespacio a lo largo de los últimos veinte años.

En este orden de ideas, la muestra utilizada son las Estrategias Nacionales de Ciberseguridad (ENC). Dado que estas estrategias constituyen el marco diseñado por el gobierno de Estados Unidos para proteger la ICN frente a las amenazas y desafíos del ciberespacio. Además, representa el núcleo del análisis de la investigación, ya que permite observar las configuraciones que ha experimentado entre 2003 y 2023. Asimismo, la unidad de análisis de esta investigación está compuesta por las cuatro (4) ENC emitidas durante las administraciones de George W. Bush, Barack Obama, Donald Trump y Joe Biden. Cada una de estas estrategias refleja los procesos de securitización de sus respectivos gobiernos en respuesta a las amenazas y desafíos del ciberespacio. La técnica empleada en esta investigación es la recopilación de documentos, que implica la recolección y análisis sistemático de las ENC. Esta técnica facilita el acceso a los contextos presentes en las ENC en relación con la protección de la ICN. Esto permite llevar a cabo un análisis exhaustivo para identificar los patrones discursivos y configuraciones de estos documentos. Por último, la fuente de datos utilizada en esta investigación es secundaria, ya que se basa en las ENC, documentos previamente elaborados por el gobierno de Estados Unidos.

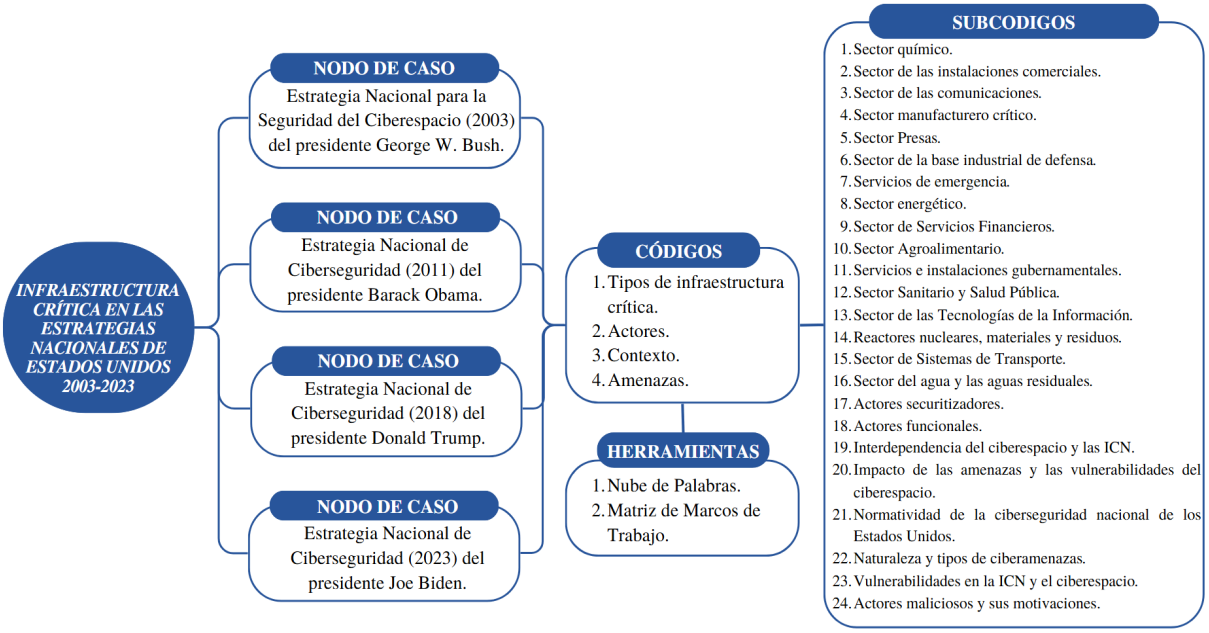
Para el desarrollo de esta investigación, se aplicará un diseño metodológico basado en el *análisis de contenido*, el cual permite la interpretación de documentos como las ENC que, al ser leídos e interpretados adecuadamente, brindan la oportunidad de conocer y comprender

diversos aspectos y fenómenos de la vida social (cfr. Andréu, 2019). En este sentido, se utiliza "la lectura (textual o visual) como instrumento de recogida de información; lectura que, a diferencia de la lectura común, debe realizarse siguiendo el método científico; es decir, debe ser sistemática, objetiva, replicable y válida" (Andréu, 2019, p. 2). Para este caso, el *análisis de contenido* ofrece una descripción objetiva, sistemática y cualitativa del contenido presente en las ENC. Esto implica la producción de datos y la interpretación de los mismos para identificar la información sustraída de las cuatro (4) categorías conceptuales establecidas.

Para realizar este análisis, se empleará el *software NVivo*, el cual "permite organizar, analizar y visualizar los datos subidos al programa, encontrando los patrones que contienen" (NVivo, 2024). En el contexto de esta investigación, el *software* facilita la organización, codificación, análisis e interpretación de las ENC. Esto permite localizar en el texto las categorías de análisis en forma de patrones, lo que a su vez posibilita la creación de matrices que expliquen cómo se han configurado las ENC en respuesta a las amenazas y desafíos del ciberespacio en relación con la ICN entre 2003 y 2023.

Para hacer el *análisis de contenido*, se utilizó el software *NVivo* de la siguiente manera (ver Gráfica 1): se creó un proyecto titulado "*Infraestructura Crítica en las Estrategias Nacionales de Estados Unidos 2003-2023*", en el cual se importaron los documentos oficiales de las cuatro (4) ENC emitidas por la Casa Blanca durante este periodo de tiempo.

FIGURA 1. ***PROCESO DE ANÁLISIS DE CONTENIDO EN EL SOFTWARE NVIVO***



Fuente: Elaboración propia con base en el proceso desarrollado en el *Software NVIVO*.

Estos documentos se asignaron al *nodo de caso* que representa las unidades de análisis observadas. Posteriormente, se establecieron cuatro (4) códigos basados en las categorías definidas en el marco teórico: **tipos de infraestructura crítica, actores, contexto y amenazas**. Dentro de cada código, se crearon subcódigos correspondientes a las subcategorías anteriormente expuestas. Por ejemplo, en la categoría de *"actores"* se incluyeron los subcódigos de *"actores securitizadores"* y *"actores funcionales"*. Una vez definida la estructura de los códigos, se inició el proceso de codificación, el cual consistió en leer detenidamente las cuatro (4) ENC. Durante esta etapa, se identificaron párrafos y oraciones que hicieran referencia a las categorías y subcategorías, asignándolas al código y subcódigo correspondiente.

Para el análisis de la información recolectada, se utilizaron dos herramientas de *NVivo* con el objetivo de aplicar la teoría de la securitización al estudio de las ENC. Este análisis se desarrolló desde dos perspectivas complementarias. En primer lugar, se realizó una aproximación general basada en las cuatro (4) categorías analíticas con el fin de identificar la construcción discursiva de los documentos. Esta etapa permitió determinar qué actores son legitimados como securitizadores y funcionales, qué amenazas son priorizadas y qué ICN se consideran estratégicas para su protección. Para ello, se empleó la herramienta de **nube de palabras**, que facilitó la visualización de la frecuencia de términos en cada categoría, lo que permitió identificar los discursos dominantes y proporcionar una visión panorámica del contenido de las ENC.

En segundo lugar, se llevó a cabo un análisis específico del proceso intersubjetivo de securitización en cada una de las ENC. Para ello, se estructuró la información en función de las cuatro (4) categorías mencionadas, con el propósito de examinar las transformaciones discursivas a lo largo del periodo de estudio. En esta fase se utilizó una **matriz de marcos de trabajo**, la cual permitió organizar y sintetizar la información de forma sistemática para identificar la recurrencia o ausencia de categorías y subcategorías en cada documento. Esta metodología posibilitó evaluar la transformación del discurso de securitización y su aplicación en la formulación de políticas orientadas a la protección de las ICN.

IV. Ciberseguridad en clave securitizadora: una mirada a las ENC de 2003 a 2023

El proceso de codificación que permitió obtener los resultados presentados se basó en la selección manual de oraciones y párrafos relevantes de las cuatro (4) ENC, las cuales fueron

clasificadas conforme a las cuatro (4) categorías analíticas y sus 24 subcategorías previamente definidas. Como resultado, se identificaron un total de 959 fragmentos codificados: 67 correspondieron a la categoría ***tipos de infraestructura crítica (types of critical infrastructure),*** 496 a ***actores (actors)***, 109 a ***contexto (context)*** y 287 a ***amenazas***. Con el fin de interpretar estos hallazgos, se desarrollará un análisis tanto general como específico, orientado al cumplimiento de los objetivos planteados en la investigación.

En primer lugar, se realizó una aproximación general a partir de las cuatro (4) categorías analíticas, con el objetivo de identificar la construcción discursiva presente en las cuatro (4) ENC. En lo que respecta a la categoría **tipos de infraestructura crítica (*types of critical infrastructure)***, entendida como el *objeto de referencia* que requiere protección frente a amenazas existenciales, se identificaron 67 referencias codificadas. Según el análisis de la nube de palabras (ver Figura 2) y las subcategorías establecidas (ver Tabla 1), las más recurrentes fueron: el sector energético (18 menciones con la palabra "energía"), los servicios e instalaciones gubernamentales (18 menciones con la palabra "gobierno"), el sector de las comunicaciones (18 menciones con la palabra "telecomunicaciones") y el sector de transporte (16 menciones con la palabra "transporte").

A partir de la perspectiva de la teoría de la securitización, que sostiene que el lenguaje configura la realidad, puede afirmarse que las ENC no se limitan a enunciar hechos, sino que participan activamente en la construcción de significados y prioridades securitarias. En este marco, cuando las ENC designan a ciertas ICN como preponderantes, están realizando un acto ilocucionario de clasificación securitaria. En otras palabras, al declarar que un sector constituye una ICN primordial, no solo informan sobre su relevancia, sino que lo constituyen como un *objeto de referencia* que merece protección prioritaria dentro del campo de la ciberseguridad. Este tipo de enunciado corresponde a un acto de habla declarativo, en tanto genera efectos concretos en la formulación e implementación de las medidas contenidas en las ENC. La priorización de sectores como la energía, el gobierno, las telecomunicaciones y el transporte, ejemplifica cómo estos actos de habla otorgan una jerarquía ontológica a determinadas ICN en el universo discursivo de la ciberseguridad nacional de Estados Unidos. En contraste, la escasa mención de sectores como el químico, sanitario, de salud pública, de aguas y aguas residuales, financiero, alimentario y agrícola, así como la total omisión de otros nueve sectores (ver Tabla 1), puede interpretarse como un acto perlocucionario negativo, cuya consecuencia es la invisibilización, marginación o desatención institucional de

dichos sectores, producto de una omisión discursiva con efectos materiales en el ámbito de la formulación e implementación de las ENC.

Figura 2. ***Nube de Palabras de la Categoría de Tipos de Infraestructura Crítica (Types of Critical Infraestructure)***

Fuente: Elaboración propia con base en los datos obtenidos de la consulta de Nube de Palabras del Software *NVivo*.

En relación con la categoría de ***actores* (*actors*)**, encargados de intervenir en los procesos de securitización mediante la formulación discursiva de amenazas, se evidenció una particularidad relevante: esta categoría concentra más del 50 % del total de códigos identificados (496 de 959). Este predominio sugiere que las ENC otorgan un papel central a los actores involucrados en la configuración y gestión de la ciberseguridad nacional. Según el análisis de la nube de palabras (ver Figura 3), los actores con mayor presencia discursiva son el gobierno (195 menciones), el gobierno federal (177 menciones), el sector privado (120 menciones), las agencias (64 menciones) y el sector público (48 menciones).

Desde la teoría de la securitización, el proceso mediante el cual un asunto previamente apolítico es transformado en un problema de seguridad implica una operación discursiva ejercida por un actor con autoridad —el *actor securitizador*— que forma parte de la élite política. Este actor identifica un *objeto de referencia* —en este caso, las ICN— y, mediante enunciados declarativos, lo constituye como un bien vulnerable frente a una amenaza inminente, al legitimar con ello la adopción de medidas extraordinarias para su protección (Peña-Galindo, 2023). En el marco de las ENC, los principales *actores securitizadores* son el

gobierno federal, las agencias de seguridad y el sector público, cuya autoridad discursiva permite delimitar no sólo qué debe ser protegido, sino también qué se considera amenaza, y bajo qué criterios.

En contraste, el sector privado se configura como el principal *actor funcional* en el ámbito de la ciberseguridad. Aunque carece del poder necesario para transformar discursivamente un asunto en una cuestión de seguridad, su rol resulta indispensable en la operativización de las medidas propuestas en las ENC. Como señalan Lostri et al. (2022), el sector privado desempeña un papel esencial en la mejora de las capacidades de ciberseguridad mediante mecanismos de intercambio de información no solo con el gobierno, sino también entre proveedores y con organismos como el DHS. Esta cooperación amplía la visibilidad del panorama de amenazas y fortalece los vínculos intersectoriales, lo que evidencia que, si bien el sector privado no define discursivamente lo que debe ser securitizado, sí contribuye materialmente a la consolidación del régimen securitario establecido.

Figura 3. ***Nube de Palabras de la Categoría de Actores (Actors)***

Fuente: Elaboración propia con base en los datos obtenidos de la consulta de Nube de Palabras del Software *NVivo*.

La categoría ***contexto*** (***context***, 109 referencias) funciona como el marco espacio-temporal en el que se configuran los procesos de securitización, así como la percepción de amenazas y la definición del *objeto de referencia* que requiere protección. En este sentido, las ENC revelan la complejidad del ciberespacio y la naturaleza dinámica y transformadora de las amenazas emergentes. El análisis de la nube de palabras (ver Figura 4) muestra que los términos más

frecuentes dentro de esta categoría son *ciberespacio* (40 menciones), *estados* (33 menciones), *sistemas* (25 menciones), *red* (17 menciones), *ataques* (16 menciones) y *actores maliciosos* (15 menciones).

A través de la interpretación de la teoría de la securitización, los enunciados presentes en las ENC no solo cumplen una función descriptiva del ciberespacio, sino que también constituyen ciertas realidades como amenazas urgentes y priorizadas. En este sentido, el lenguaje técnico y normativo que caracteriza el discurso de las ENC —en particular, la reiteración de términos como "red" y "sistemas"— debe entenderse como una forma de acto declarativo que contribuye a la construcción institucional de un escenario securitizado. Adicional a esto, la enunciación de los "ataques" y "actores maliciosos" permite movilizar medidas excepcionales bajo la legitimidad del interés nacional al determinarlos como peligros inminentes. Esta práctica discursiva no es neutra: responde a una lógica en la que los *actores securitizadores* definen selectivamente qué agentes son considerados peligrosos y qué consecuencias potenciales merecen atención prioritaria. Así, las prioridades estratégicas enunciadas en las ENC están determinadas no solo por un análisis técnico del riesgo, sino por una operación discursiva que configura el campo de lo visible, lo legítimo y lo urgente en materia de ciberseguridad, dejando fuera otras posibles amenazas o actores que no se ajustan a dicha narrativa.

Figura 4. ***Nube de Palabras de la Categoría de Contexto (Context)***

Fuente: Elaboración propia con base en los datos obtenidos de la consulta de Nube de Palabras del Software *NVivo*.

El análisis de la categoría ***amenazas* (*threats*)** resulta fundamental para comprender la construcción discursiva del "enemigo" desde una perspectiva schmittiana, en la medida en que las amenazas actúan como justificación para la formulación y legitimación de las ENC. De acuerdo con el análisis de la nube de palabras (ver Figura 5), los términos más recurrentes en esta categoría son *ataques cibernéticos* (62 menciones), *actores maliciosos* (51), *estados* (48), *vulnerabilidades* (30) y *ransomware* (25).

Si bien los ciberataques, las vulnerabilidades o el *ransomware* no constituyen enemigos en un sentido schmittiano estricto —es decir, no son sujetos concretos que puedan ser reconocidos, diferenciados y combatidos por su hostilidad explícita hacia un "nosotros" político—, el análisis discursivo de las ENC sugiere una reconstrucción de la lógica amigo-enemigo a partir de la representación de ciertos actores como amenazas ontológicas. En este contexto, la alta frecuencia léxica de términos como "ataques cibernéticos", "*ransomware"* y "actores maliciosos" opera como una forma de delimitación simbólica entre un orden que debe ser protegido y una alteridad que lo pone en riesgo. Tal como señala Aslan (2023, p. 21), la popularización del concepto de ciberataques refleja una narrativa en la que la seguridad nacional se concibe bajo una lógica de excepcionalidad constante. Particularmente, cuando las ENC aluden a actores maliciosos y a la participación de ciertos Estados en actividades cibernéticas hostiles, se configura un marco discursivo que identifica sujetos concretos como potenciales enemigos. Esta operación discursiva reproduce, aunque de forma matizada, la lógica schmittiana de la política como una distinción fundamental entre amigos y enemigos: no en términos tradicionales de conflicto bélico, sino en una forma adaptada al escenario digital, donde la hostilidad se articula a través de riesgos tecnológicos que adquieren agencia discursiva. Así, el "enemigo" no es solo quien ataca, sino aquel a quien se le adjudica la capacidad intencional de comprometer la soberanía digital del Estado, lo que justifica tanto la securitización del ciberespacio como la adopción de medidas extraordinarias.

Figura 5. ***Nube de Palabras de la Categoría de Amenazas (Threats)***

Fuente: Elaboración propia con base en los datos obtenidos de la consulta de Nube de Palabras del Software *NVivo*.

En suma, el análisis general de las ENC a partir de las cuatro (4) categorías establecidas permitió evidenciar cómo el lenguaje desempeña un papel constitutivo en la construcción del campo securitario de la ciberseguridad en Estados Unidos. Desde la teoría de la securitización, las ENC no deben leerse únicamente como documentos técnicos o normativos, sino como prácticas discursivas que configuran realidades políticas, al identificar objetos de referencia, actores securitizadores y funcionales, y amenazas existenciales. En este sentido, la identificación de ciertas ICN, la centralidad del gobierno federal como actor securitizador, la delimitación de contextos de riesgo asociados al ciberespacio, y la clasificación de amenazas —particularmente de actores maliciosos y Estados hostiles—, constituyen actos de habla que no sólo describen una situación de inseguridad, sino que la instauran como tal, al legitimar con ello la adopción de las medidas instauradas en las ENC.

En segundo lugar, se desarrolló un análisis específico de las cuatro (4) categorías analíticas con el propósito de observar las transformaciones discursivas en las ENC a lo largo de los últimos veinte años. Este análisis se apoyó en el uso de una matriz de marcos de trabajo (ver Tabla 2), la cual permitió identificar las variaciones de los procesos de securitización de las ENC. Sin embargo, para fortalecer los resultados derivados de la matriz, se va a comparar cada ENC para identificar las transformaciones del discurso securitario en función de las

similitudes y diferencias en la forma en que se nombran, significan y representan las ICN, los actores, el contexto y las amenazas.

En torno a la categoría ***tipos de infraestructura crítica* (*types of critical infrastructure*)**, la transformación entre los periodos presidenciales se evidencia en las variaciones discursivas que cada administración imprime en la definición de los sectores considerados como ICN y las visiones subyacentes de seguridad de cada ENC. En 2003, la administración de Bush configuró un discurso securitizador con una orientación marcadamente realista, al priorizar la protección de ICN tradicionalmente vinculadas a la defensa nacional, la estabilidad económica y el funcionamiento esencial del Estado (base industrial de defensa, transporte, tecnologías de la información, telecomunicaciones, servicios de emergencia, salud pública y productos químicos). La exclusión discursiva de las instalaciones comerciales, la manufactura crítica y las presas relega dichas ICN fuera del campo de lo visible y de lo urgente. Esta orientación refleja una concepción convencional de la ciberseguridad como defensa frente a amenazas externas, alineada con los postulados del realismo político, donde el Estado se constituye como el actor central frente a peligros geopolíticos definidos.

En 2011, la administración de Obama reconfiguró parcialmente el discurso securitizador al ampliar el espectro de las ICN priorizadas, al incorporar las comunicaciones, los servicios energéticos y el sistema financiero. Esta ampliación refleja un acto ilocucionario que redefine el *objeto de referencia* al reconocer nuevas formas de vulnerabilidad en sectores altamente interconectados y expuestos a amenazas. No obstante, esta transformación discursiva no implicó una ruptura sustantiva con la lógica estadocéntrica heredada, ya que el eje articulador del discurso siguió siendo la protección del Estado frente a amenazas originadas en actores estatales. Lo que se evidencia en la omisión de sectores como las instalaciones comerciales o el nuclear, cuya exclusión implica un acto perlocucionario de marginación, que limita su visibilidad dentro de la ciberseguridad.

Esta tendencia continuó en 2018 con la administración de Trump, en la que se consolidó un enfoque securitizador altamente selectivo, orientado hacia infraestructuras cuya interrupción supondría un impacto inmediato y tangible en la seguridad nacional, tales como los sectores de energía, finanzas, telecomunicaciones y transporte. Esta priorización refleja una lógica securitaria centrada en la inmediatez del daño y en la protección de activos estratégicos del aparato estatal y económico. En consecuencia, ICN fundamentales para la seguridad humana —como el agua, los servicios de emergencia o la producción alimentaria— fueron

subordinados. Esta omisión implica una visión reduccionista de la ciberseguridad, que desatiende la complejidad y transversalidad de las amenazas en favor de una jerarquización funcional de las infraestructuras según su valor estratégico para la defensa nacional.

Finalmente, en 2023, bajo la administración de Biden, se introdujo un enfoque discursivo orientado a la resiliencia digital, al reconocer la creciente interdependencia tecnológica y la sofisticación de las amenazas cibernéticas. Si bien este enfoque representa un avance en términos de reconocimiento de la transformación digital como vector de riesgo, persiste una lógica jerárquica que privilegia ciertos sectores (energía, TIC, salud, agua y transporte) y margina otros (químico, instalaciones comerciales y bases industriales de defensa), sin incorporar plenamente una noción multidimensional de la ciberseguridad.

En conjunto, las cuatro (4) ENC han identificado a las ICN como *objetos de referencia* cuya protección resulta esencial para garantizar la estabilidad y continuidad del Estado. No obstante, de los 16 sectores oficialmente reconocidos como ICN (ver Tabla 1), no todos han sido mencionados de forma explícita y sistemática en cada estrategia, lo que revela una selección discursiva que responde a construcciones específicas de riesgo y necesidad. Desde la securitización, las decisiones sobre qué tipos de ICN securitizar —y cuáles omitir— no solo responden a contextos geopolíticos, económicos y tecnológicos particulares, sino que parten de las visiones estratégicas que pretenda establecer cada administración.

En relación con la categoría **actores (*actors*)**, los *actores securitizadores* y *funcionales* han experimentado transformaciones sustanciales en las narrativas que promueven y en las funciones que desempeñan dentro de las ENC. En particular, los *actores securitizadores* han legitimado su autoridad mediante actos de habla que configuran el discurso sobre la ciberseguridad. Esta legitimidad no se genera en un vacío ni de manera neutral, sino que se produce a partir de sus trayectorias institucionales y experiencias previas (Peña-Galindo, 2024). En este contexto, la ENC de 2003, bajo la administración de Bush, consolidó al gobierno federal y al recién creado Departamento de Seguridad Nacional (DHS) como los principales órganos rectores del proceso de securitización del ciberespacio. Su discurso, fuertemente anclado en una lógica de defensa nacional, otorgó a los niveles estatal y local directrices claras para actuar bajo un marco de protección de las ICN.

En 2011, bajo la administración Obama, los *actores securitizadores* —compuestos por los niveles federal, estatal y local del gobierno— expandieron el alcance del proceso de

securitización al redefinir la ciberseguridad no solo como un asunto de seguridad nacional, sino también como una cuestión estratégica vinculada a la estabilidad económica del país. Esta ampliación discursiva introdujo un lenguaje que asoció la ciberseguridad con la competitividad global y la innovación tecnológica.

Durante el mandato de Trump en 2018, los *actores securitizadores* continuaron siendo el gobierno federal, junto con los niveles estatal y local; sin embargo, el discurso securitizador adquirió un tono marcadamente confrontativo, que intensificó la dicotomía amigo-enemigo de schmitt. Este giro retórico se tradujo en una narrativa de amenaza permanente, centrada en actores estatales adversarios, lo cual legitimó a la comunidad de inteligencia y el Departamento de Defensa como actores securitizadores en la configuración de las ENC.

La ENC de 2023, formulada durante la administración Biden, mantuvo al gobierno federal, estatal y local como los principales *actores securitizadores.* No obstante, introdujo un giro discursivo hacia una visión más colaborativa que amplía la participación de aliados internacionales y sectores estratégicos estatales. Esta reformulación narrativa se expresa mediante actos de habla orientados a redistribuir la responsabilidad de la protección cibernética. Si bien esta aproximación representa una ruptura parcial con las formas de securitización centradas exclusivamente en el Estado, continúa reproduciendo jerarquías de poder al conservar al gobierno federal como núcleo articulador del discurso y la acción securitizadora.

En relación a los *actores funcionales*, han mantenido una presencia constante en las ENC, aunque con variaciones en su visibilidad y grado de responsabilidad. En 2003, bajo una lógica liberal de gobernanza, el sector privado (empresas y organizaciones) fue concebido como un pilar estratégico mediante un enfoque de adopción de estándares de seguridad. Esta narrativa posicionó a las empresas como socios indispensables del Estado, al legitimar un modelo de colaboración público-privada que perduraría como eje estructurante del discurso securitizador posterior. En 2011, la administración Obama amplió los *actores funcionales* al incluir la alianza estratégica entre agencias gubernamentales, empresas tecnológicas y actores internacionales. Este fortalecimiento de la cooperación intersectorial se articuló mediante un discurso securitizador que incorporó elementos de competitividad, innovación y desarrollo económico. De este modo, el proceso securitizador se vuelve más complejo y transnacional, al articular los regímenes, organizaciones e instituciones internacionales para la cooperación internacional (Higuera, 2019).

Durante el mandato de Trump en 2018, el sector privado fue objeto de una reconfiguración normativa, al ser interpelado como corresponsable de proteger las ICN. Si bien no detentaba poder decisorio, fue investido como un consejero estratégico clave dentro del proceso securitizador, a partir de una narrativa de corresponsabilidad que intensificó su grado de compromiso operativo. La ENC de 2023, bajo la administración Biden, representó un giro discursivo significativo al promover una concepción de la ciberseguridad como bien público. Este nuevo marco discursivo desplazó el énfasis de la autorregulación hacia una protección del ciberespacio concebida como una responsabilidad colectiva que compromete al Estado y, a las pequeñas y a las grandes corporaciones tecnológicas.

En resumen, los *actores securitizadores* y *funcionales* han experimentado transformaciones discursivas que reflejan la evolución del proceso de securitización del ciberespacio. Aunque el gobierno federal ha mantenido su rol central como autoridad legítima en materia de ciberseguridad, se han incorporado nuevas narrativas que incorporan a los estados y al sector privado como actores funcionales. Sin embargo, estas reformulaciones, si bien introducen matices colaborativos, continúan reproduciendo jerarquías de poder donde el Estado actúa como núcleo articulador del discurso securitizador.

Desde la teoría de la securitización y el enfoque socio-cognitivo de van Dijk, el **contexto *(context)*** en las ENC no debe entenderse únicamente como un entorno técnico-operativo que condiciona las acciones institucionales, sino como una construcción discursiva que articula modelos mentales compartidos con compromisos ideológicos e institucionales. Esta perspectiva permite reconocer que las ENC no solo describen un escenario del ciberespacio, sino que lo configuran discursivamente a través de marcos cognitivos que interpretan dicho entorno como un dominio de amenaza constante. Así, el discurso securitizador produce una narrativa donde la vulnerabilidad del ciberespacio y de las ICN se presenta como una justificación legítima para la intervención del Estado. Esta lógica, propia del proceso de securitización, se sostiene en una triangulación entre cognición, contexto y discurso, donde la representación del riesgo se convierte en un acto performativo que redefine lo que debe ser protegido, quién debe hacerlo y bajo qué mecanismos.

Históricamente, el contexto en las ENC se ha transformado al compás de los cambios tecnológicos, políticos y estratégicos que consolidan al ciberespacio como un componente estructural de la seguridad nacional. Desde 2003, se advierte sobre la creciente digitalización de la economía, la administración pública y la vida cotidiana, al enfatizar la necesidad de

cooperación público-privada. Para 2011, la interdependencia global del ciberespacio y la emergencia de actores no estatales reconfiguran el discurso hacia la flexibilidad estratégica. En 2018, la securitización se intensifica al centrarse en la competencia geopolítica, la agresividad de otros actores estatales y al priorizar la disuasión frente a los ataques cibernéticos. Finalmente, en 2023, se institucionaliza un marco de gobernanza integral basado en la Estrategia de Confianza Cero y en la obligación regulatoria de proteger las ICN. Este recorrido evidencia que la securitización no ha sido estática, sino que ha respondido a la transformación progresiva del contexto mediante un discurso que traduce los desafíos tecnológicos en amenazas existenciales para el Estado.

En este marco, las amenazas y vulnerabilidades del ciberespacio han dejado de ser percibidas como meros problemas técnicos para convertirse en factores estructurantes de la política de seguridad nacional. La dificultad de atribución en los ciberataques (2003), la explotación de la interdependencia de las ICN por actores hostiles (2011), la escala creciente de intrusiones (2018) y la insuficiencia de las medidas voluntarias de protección (2023), han impulsado una narrativa que refuerza la urgencia de respuestas estatales robustas. Esta narrativa, a su vez, legitima el desarrollo de un marco normativo cada vez más riguroso, como lo demuestran la Orden Ejecutiva 13231 (2001), la adopción del enfoque de Confianza Cero (2021) y los nuevos estándares regulatorios propuestos en 2023 para sectores críticos. En suma, el contexto ha sido simultáneamente moldeado y constituido del discurso de securitización, lo que evidencia que la representación discursiva es fundamental para comprender el modo en que el ciberespacio se ha integrado a las lógicas de protección del orden estatal.

La categoría de **amenazas (*threats*)** en las ENC revelan un proceso de complejización y expansión discursiva, en el cual los actos de habla que definen los riesgos cibernéticos se han transformado conforme a los cambios tecnológicos, geopolíticos y estratégicos. En términos securitizadores, las amenazas son construcciones discursivas que configuran una narrativa sobre lo que debe ser protegido como un referente existencial, y legitiman acciones extraordinarias por parte del Estado. En 2003, bajo la administración Bush, el discurso se centró en amenazas técnicas como *malware, ransomware* y ataques *DDoS*, concebidos como desafíos operativos a la ICN. Para 2011, con la administración Obama, el espectro de amenazas se amplió al incluir fenómenos como el ciberespionaje, la interferencia en procesos electorales y la convergencia entre ciberterrorismo y ciberdelincuencia, lo cual refleja una reconfiguración discursiva que vincula la seguridad cibernética con la estabilidad

institucional y económica del país. En 2018, bajo el mandato de Trump, el discurso securitizador adoptó un tono más confrontativo, centrado en el espionaje económico, la manipulación de datos y la amenaza constante de actores estatales adversarios —como Rusia, China, Irán y Corea del Norte— lo que refuerza una narrativa de amigo-enemigo. En 2023, la administración Biden profundizó esta línea discursiva al advertir sobre amenazas avanzadas, como el uso de inteligencia artificial y técnicas automatizadas por parte de Estados-nación, destacando así la sofisticación creciente de los adversarios.

De manera paralela, cada ENC ha incorporado las *vulnerabilidades* como un elemento clave dentro del proceso de securitización, ya que estas debilidades se constituyen como condiciones facilitadoras del riesgo. En 2003, se señaló la ausencia de seguridad desde el diseño, el uso masivo de *software* desactualizado y la carencia de una cultura de ciberseguridad. En 2011, la narrativa se desplazó hacia la interdependencia de los sistemas digitales y la falta de coordinación efectiva entre actores públicos y privados. En 2018, se identificaron nuevos factores críticos como la obsolescencia tecnológica, la dependencia de proveedores externos y la debilidad regulatoria. Finalmente, en 2023, se reconocieron desafíos como la opacidad de las cadenas de suministro digitales, la proliferación de dispositivos IoT inseguros, la automatización de los ataques y la insuficiencia de capacitación especializada en sectores estratégicos.

Asimismo, los actores maliciosos y sus motivaciones han sido objeto de una construcción discursiva que refleja tanto la diversificación de las amenazas como el reacomodo del tablero geopolítico. En 2003, predominaban actores no estatales con motivaciones económicas; sin embargo, a partir de 2011, la inclusión explícita de actores estatales como Rusia y China implicó una reformulación del marco securitizador, en el que el ciberespacio dejó de ser visto exclusivamente como un ámbito de criminalidad para entenderse también como un terreno de confrontación entre Estados. En 2023, esta narrativa se complejiza aún más al reconocer la cooperación entre actores estatales y organizaciones criminales como *proxies*, lo que dificulta la atribución de responsabilidades y legítima medidas más amplias de vigilancia, defensa y disuasión.

En suma, la transformación de la categoría amenazas refleja un proceso de securitización gradual y multifacético, en el cual se amplía la naturaleza de los riesgos, se diversifican los actores involucrados y se legitiman respuestas estratégicas más integrales. Este proceso discursivo no sólo configura una percepción de vulnerabilidad persistente, sino que también

justifica la expansión del poder estatal y la articulación de nuevos marcos normativos, institucionales y tecnológicos para la defensa del ciberespacio como un referente existencial de la ciberseguridad nacional.

Tabla 2. ***Configuración de las ENC de Estados Unidos en respuesta a las amenazas y desafíos del ciberespacio, en relación a la ICN entre 2003 a 2023***

	ENC (2003) George W. Bush	ENC (2011) Barack Obama	ENC (2018) Donald Trump	ENC (2023) Joe Biden
Tipos de Infraestructura Crítica (*Types of Critical Infraestructure*)	Se enfocó en la protección de las ICN tradicionalmente relacionadas con la seguridad nacional y la estabilidad económica, pero sectores como instalaciones comerciales, manufactura crítica y presas no fueron mencionados.	Se amplía la protección a sectores como comunicaciones, servicios financieros y energéticos, además de los mencionados en la ENC de 2003. Sin embargo, persisten vacíos en sectores como el nuclear y las instalaciones comerciales.	Se prioriza la protección de sectores críticos con impacto directo en la seguridad nacional (energía, finanzas, transporte y TIC), mientras que sectores como el agroalimentario, servicios de emergencia y agua quedan relegados.	Se adopta un enfoque integral de resiliencia, al priorizar sectores clave como energía, TIC, salud, agua y transporte. Sin embargo, sectores menos digitalizados como el químico, instalaciones comerciales y bases industriales de defensa no se tratan con profundidad.
Actores (*Actors*)	**Actores securitizadores:** Gobierno federal y DHS, en colaboración con gobiernos estatales y locales, para fortalecer la ciberseguridad. **Actores funcionales:** Sector privado (empresas y organizaciones), que desempeña un papel clave a través de la adopción de medidas de seguridad.	**Actores securitizadores:** Gobierno federal, estatal y local, que definen la ciberseguridad como un asunto de seguridad nacional y económica. **Actores funcionales:** Incluyen la cooperación con las agencias gubernamentales, las empresas tecnológicas y los aliados internacionales.	**Actores securitizadores:** Gobierno federal, estatal y local, junto con el Departamento de Defensa y la comunidad de inteligencia. **Actores funcionales:** Sector privado, responsable de proteger datos y infraestructuras críticas, al actuar como consejeros estratégicos en ciberseguridad.	**Actores securitizadores:** Gobierno federal, estatal y local, que implementan modelos colaborativos con otros estados y sectores estratégicos. **Actores funcionales:** Redistribuyen la carga de ciberseguridad, pasando de individuos a pequeñas empresas en conjunto con grandes corporaciones y el gobierno federal.
Contexto (*Context*)	Se destaca la creciente digitalización de la economía, la administración pública y la vida cotidiana, al posicionar al ciberespacio como un pilar estructural del Estado. Se enfatiza la cooperación público-privada para gestionar riesgos cibernéticos.	Se resalta la importancia del ciberespacio para Estados Unidos y la necesidad de un enfoque adaptativo ante actores no estatales. Se resalta la interdependencia global del ciberespacio y se subraya la vulnerabilidad de las ICN debido a su fragmentación.	Se destaca la competencia geopolítica y la agresividad de actores estatales, al priorizar la disuasión frente a los ataques cibernéticos. Se identifica como una vulnerabilidad clave la obsolescencia de las infraestructuras tecnológicas.	Se establece una regulación más estricta y un marco de gobernanza integral, al enfatizar la protección obligatoria de ICN y la implementación de la Estrategia de Confianza Cero para fortalecer la seguridad del ciberespacio.
Amenazas (*Threats*)	Las principales amenazas identificadas fueron el *malware*, *ransomware* y ataques *DDos*. Las vulnerabilidades fueron la falta de seguridad en el diseño de sistemas y una cultura de ciberseguridad deficiente. Los actores maliciosos fueron los no estatales que buscan beneficios económicos.	Se amplía el espectro de amenazas cibernéticas , al incluir el ciberespionaje, manipulación electoral y ciberterrorismo. La interdependencia de los sistemas digitales se reconoce como un factor de riesgo significativo. Los actores maliciosos clave fueron Rusia, China, Irán y Corea del Norte.	Las amenazas principales fueron el ciberespionaje económico y la manipulación de datos. La obsolescencia tecnológica y la falta de regulación aumentan la exposición a riesgos. Los principales actores estatales hostiles en el ciberespacio fueron Rusia, China e Irán.	Se destacan amenazas como el ciberespionaje y ataques basados en inteligencia artificial. La falta de control en las cadenas de suministro digitales representa una vulnerabilidad crítica. Los actores maliciosos fueron las organizaciones criminales y actores estatales.

Fuente: Elaboración propia con base en los datos obtenidos de la matriz de marcos de trabajo del software *NVivo*.

En ese sentido, entre 2003 y 2023, las ENC en Estados Unidos se configuraron como respuestas cada vez más sofisticadas frente a amenazas emergentes en el ciberespacio, a través de un proceso de securitización que articula actores, contextos, amenazas e ICN mediante discursos adaptativos al entorno geopolítico y tecnológico de cada administración, como se esquematiza en la tabla 2. Inicialmente basadas en una lógica realista y estadocéntrica, las ENC se transformaron hacia una concepción más compleja y colaborativa de la ciberseguridad, al incorporar nociones de resiliencia digital, corresponsabilidad público-privada y amenazas avanzadas. Esta transformación discursiva redefinió tanto los *objetos de referencia* (ICN priorizadas) como los sujetos legitimados para actuar (*actores securitizadores* y *funcionales)*, al ampliar la narrativa desde la defensa nacional hacia una ciberseguridad que responda a las amenazas y riesgos cibernéticos del país.

V. Conclusiones

Las ENC de Estados Unidos entre 2003 y 2023 constituyen un instrumento clave en el proceso de securitización del ciberespacio, al configurar un discurso estatal que redefine las amenazas, construye referentes de seguridad y legítima la defensa de las ICN. Su transformación evidencia un marco adaptativo en el que convergen tres tendencias. La primera es la creciente sofisticación y diversificación de las amenazas cibernéticas, especialmente visible en la estrategia de 2023, que introduce riesgos asociados al espionaje estatal, al uso de inteligencia artificial y a la automatización de ciberataques. Este desplazamiento desde ataques técnicos convencionales hacia amenazas más complejas y geopolíticamente sensibles ha demandado la expansión del repertorio securitizador y la adopción de enfoques preventivos y multidimensionales.

La segunda tendencia se manifiesta en la consolidación de actores como componentes fundamentales de la arquitectura de gobernanza cibernética. A través de actos de habla institucionalizados, el gobierno federal ha asumido un rol protagónico en la articulación del discurso securitizador, mientras que el sector privado ha sido interpelado como un aliado estratégico indispensable. Esta cooperación multisectorial no solo ha legitimado un modelo de gobernanza compartida, sino que también ha dado lugar a una narrativa de corresponsabilidad que fortalece la resiliencia operativa e institucional frente a los riesgos cibernéticos. La tercera tendencia se refiere al tratamiento de la ICN, la cual, si bien fue destacada explícitamente en la estrategia de 2003 como un eje prioritario, ha tendido a

diluirse en las estrategias posteriores, lo que revela una tensión entre su relevancia estratégica y la falta de una conceptualización sistemática dentro del marco securitizador.

Estas dinámicas permiten concluir que el proceso de securitización del ciberespacio ha estado impulsado principalmente por la identificación y amplificación discursiva de amenazas, más que por un desarrollo de las ICN. En este contexto, el rol del gobierno federal y del sector privado ha sido determinante para sostener una narrativa de legitimidad que justifica la adopción de ENC cada vez más complejas, interdependientes y adaptativas.

VI. Bibliografía

Agencia de Seguridad Cibernética y de Infraestructura (CISA). (2021). ¿Qué es la ciberseguridad? https://www.cisa.gov/news-events/news/what-cybersecurity

Agencia de Seguridad Cibernética y de Infraestructura (CISA). (2024a). Seguridad y resiliencia de infraestructura crítica. https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience

Agencia de Seguridad Cibernética y de Infraestructura (CISA). (2024b). Sectores de infraestructura crítica. https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors

Agencia de Seguridad Cibernética y de Infraestructura (CISA). (2025). Amenazas cibernéticas y avisos. https://www.cisa.gov/topics/cyber-threats-and-advisories

Andréu, J. (2019). Las técnicas de Análisis de Contenido: Una revisión actualizada. Abaco en Red. https://abacoenred.org/wp-content/uploads/2019/02/Las-t%C3%A9cnicas-de-an%C3%A1lisis-de-contenido-una-revisi%C3%B3n-actualizada.pdf

Azmi, R., Tibben, W. & Win, K. (2018). Review of Cybersecurity Frameworks: Context and Shared Concepts. *Journal of Cyber Policy*, 3:(2), 258-283,

https://www-tandfonline-com.ezproxy.unbosque.edu.co/doi/full/10.1080/23738871.2018.1520271

Buzan et al. (1998). *Security: A New Framework for Analysis.* Lynne Rienner Publishers.

Craig, A., Johnson, R. & Gallop, M. (2022). Building Cybersecurity Capacity: A Framework of Analysis for National Cybersecurity Strategies. *Journal of Cyber Policy,* 7(3), 375-398, https://www-tandfonline-com.ezproxy.unbosque.edu.co/doi/full/10.1080/23738871.2023.2178318

Demurtas, A. (2029). Veinte años de la teoría de la securitización: puntos fuertes y débiles de su operacionalización. *Revista Análisis Jurídico-Político*, 1(1), 167-187.

Granata, E. (2019). *International vs. National Cybersecurity Policy*. [Tesis de maestría]. Utica College.

Hernandez, R., Fernández, C., Baptista, P. (2014). *Metodología de la Investigación*. McGraw-Hill & Interamericana Editores.

Higuera, F. (2019). Gobernanza Global en la Cooperación Internacional y el Desarrollo: una discusión desde las Relaciones Internacionales. En: Arévalo-Ramírez, W., Escobar, C., e Higuera, F. (Comp). *Gobernanza Global y Responsabilidad Internacional del Estado. Experiencias en América Latina* (pp. 67-89). Editorial Universidad El Bosque.

Leroy, I., & Zolotaryova, I. (2023). Critical Infrastructure Defense: Perspectives from the EU and USA Cyber Experts. *Natsional'Nyi Hirnychyi Universytet. Naukovyi Visnyk,* (5), 165-170.

Lostri et al. (2022). A Shared Responsibility: Public-Private Cooperation for Cybersecurity. Center of Strategic & International Studies. https://www.csis.org/analysis/shared-responsibility-public-private-cooperation-cybersecurity

Oficina de la Responsabilidad del Gobierno de Estados Unidos (GAO). (2024). High-Risk Series: Urgent Action Needed to Address Critical Cybersecurity Challenges Facing the Nation. https://www.gao.gov/products/gao-24-107231

Oluomachi et al. (2024). Assessing The Effectiveness of Current Cybersecurity Regulations and Policies in the US. International Journal of Scientific and Research Publications, 14,(2), 78-85.

Ömer et al. (2023). A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions. Electronics, 12, 1-42.

Peña-Galindo, A. A. (2023). La priorización de la seguridad nacional en los análisis de frontera en Colombia: fuente de vulnerabilidades inexploradas. En Pastrana-Buelvas, Reith y Cabrera Ortiz: *Transición del orden mundial: Impactos en las estrategias de seguridad y defensa en Colombia y la región* (pp. 537-560). Konrad-AdenauerStiftung.

Peña-Galindo, A. A. (2024) *Monólogos del Imperio: una historiografía sobre algunos silencios en la disciplina de las Relaciones Internacionales.* Editorial Universidad El Bosque.

Sam, D. D. (2023). *The Impact of System Outages on National Critical Infrastructure Sectors: Cybersecurity Practitioners' Perspective*. [Tesis doctoral]. Marymount University.

Sánchez, M. (2005). La metodología en la investigación cualitativa. *Mundo Siglo XXI*, (1), 115-118. https://repositorio.flacsoandes.edu.ec/bitstream/10469/7413/1/REXTN-MS01-08-Sanchez.pdf

Schmitt, C. (1932). El Concepto de lo Político. En: El Concepto de lo Político (pp. 1-13). Alianza Editorial.

Shannon et al. (2003). Interdependence Across the National Critical Functions. Homeland Security Research Division.

https://www.rand.org/content/dam/rand/pubs/working_papers/WRA200/WRA210-1/RAND_WRA210-1.pdf

The White House. (2003). *The National Strategy to Secure Cyberspace*. https://www.cisa.gov/sites/default/files/publications/cyberspace_strategy.pdf

Unión Internacional de Telecomunicaciones (UIT). (2024). *Internet Use*. https://www.itu.int/itu-d/reports/statistics/2023/10/10/ff23-internet-use/

Vila, M y Marcelo, S. (2019). Ciberpolítica, digitalización y relaciones internacionales: un enfoque desde la literatura crítica de economía política internacional. *Relaciones Internacionale*s, 40, 113-132.

Voo, J., Hemani, I. & Cassidy, D. (2022). National Cyber Power Index 2022. *Belfer Center for Science and International Affairs, Harvard Kennedy School.* https://www.belfercenter.org/publication/national-cyber-power-index-2022