**Norteamérica, Revista Académica del CISAN-UNAM, año 19, número 1, enero-junio de 2024**
**DOI:** https://doi.org/10.22201/cisan.24487228e.2024.1.663
**FR:** 02/10/2023
**FA:** 19/01/2024
Versión *Ahead-of-Print*

**Ensayos**

# Rezago y asimetrías de las política nacional e internacional de ciberseguridad de México frente a Estados Unidos y Canadá: retos de cooperación para Norteamérica

Disparities and Backlogs in Mexico's National and International Cybersecurity Policies vis-à-vis the United States and Canada: Challenges of Cooperation for North America

Juan Manuel Aguilar Antonio*

**Resumen:** La investigación analiza la política nacional e internacional de ciberseguridad de Estados Unidos, México y Canadá. Se parte de la hipótesis que el perfil de política exterior activa de impacto regional e internacional, y la trayectoria histórica individual de más de dos décadas, de Estados Unidos y Canadá, explican el nivel de consolidación en el desarrollo de su política de ciberseguridad. Se realizó una revisión electica de teorías de relaciones internacionales como el realismo, liberalismo, constructivismo y teoría de la guerra para identificar elementos teóricos para el análisis de la política internacional y nacional de los tres países. Se concluye que tanto Estados Unidos, considerado una potencia global en ciberseguridad, y Canadá, potencia regional, poseen una política exterior activa en la materia, con una trayectoria de casi dos décadas. Mientras que Mexico posee un fuerte rezago en la materia que no se relaciona con una política nacional e internacional de ciberseguridad efectiva.
**Palabras Clave:** Ciberseguridad, Estados Unidos, México, Canadá, Infraestructuras Críticas, Política Nacional de Ciberseguridad, Delitos Cibernéticos, Protección de Datos.

**Abstract:** The research analyzes the national and international cybersecurity policies of the United States, Mexico, and Canada. It starts from the hypothesis that the active foreign policy profile with regional and international impact, and the individual historical trajectory of more than two decades of the United States and Canada, explain the level of consolidation in the development of their cybersecurity policy. An eclectic review of international relations theories such as realism, liberalism, constructivism, and the theory of war was conducted to identify theoretical elements for the analysis of the international and national policies of the three countries. It is concluded that both the United States, considered a global power in cybersecurity, and Canada, a regional power, have an active foreign policy in the field, with a trajectory of almost two decades. Meanwhile, Mexico has a significant lag in the field that is not related to an effective national and international cybersecurity policy.
**Keywords:** Cybersecurity, United States, Mexico, Canada, Critical Infrastructures, National Cybersecurity Policy, Cybercrimes, Data Protection.

*Este artículo se realizó con apoyo del Programa de Becas Posdoctorales de la UNAM, el autor es becario del Centro de Investigaciones sobre América del Norte (CISAN), asesorado por el Dr. Leonardo Curzio Gutiérrez, alchemistffvii@hotmail.com

**DOI:** https://doi.org/10.22201/cisan.24487228e.2024.1.663
Versión *Ahead-of-Print*

## Introducción

En 2018, el proceso de renegociación del Tratado de Libre de Comercio (TLCAN o NAFTA por sus siglas en inglés) culminó con su reestructuración en el Tratado México, Estados Unidos y Canadá (T-MEC o UMSCA). La nueva versión de este acuerdo puso sobre la mesa temas emergentes en la agenda de cooperación multilateral de América del Norte (Aguirre Quezada, 2022). En el artículo 19.15 de T-MEC, del capítulo 19 sobre comercio digital, se señala a la ciberseguridad como una amenaza que menoscaba la confianza en el intercambio económico de la región. Por lo cual, los países miembros se comprometen a desarrollar capacidades nacionales para dar respuesta a incidentes de ciberseguridad y fortalecer los mecanismos de colaboración existentes para identificar y mitigar los incidentes en las redes o infraestructuras que involucran a los tres socios (TMEC, 2023).

Este artículo reconoce la naturaleza cambiante de las amenazas a la ciberseguridad y propone que los países utilicen enfoques de análisis basados en riesgos que estén relacionados con normas consensuadas y buenas prácticas para mitigar los efectos de las amenazas cibernéticas (T-MEC, 2018). De esta forma, el artículo 19.15 del T-MEC se ha transformado en el primer marco de cooperación multilateral de ciberseguridad en Norteamérica. No obstante, la ciberseguridad representa un concepto más amplio y holístico que no se limitan al intercambio económico entre Estados Unidos, México y Canadá. En los hechos, el desarrollo de una política de ciberseguridad se ha transformado en una piedra angular para la seguridad nacional, la política exterior, el desarrollo económico y la prosperidad de los Estados-Nación en las dos primeras décadas del siglo XXI.

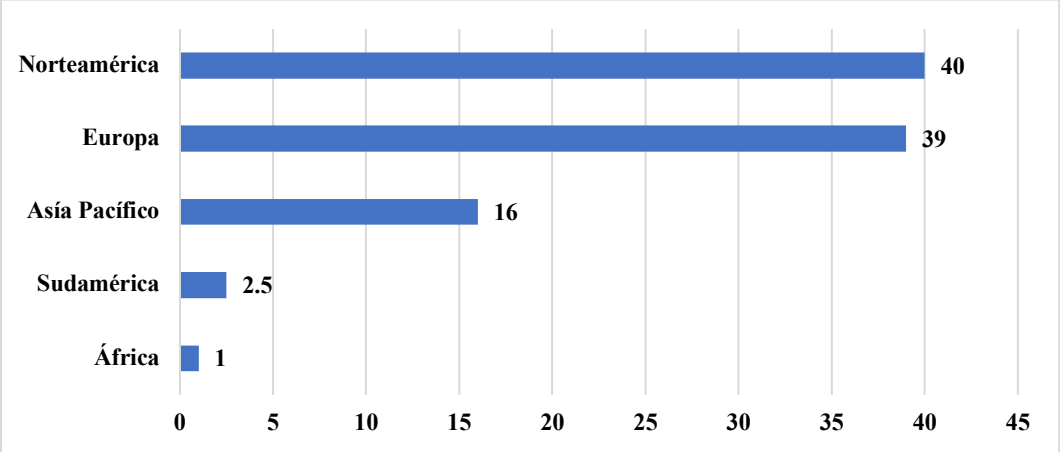
Asimismo, el avance de la digitalización, como consecuencia de la crisis global por COVID-19, impulsó la incidencia de ataques cibernéticos alrededor del mundo. Esto se relaciona con el impulso del internet que dio la pandemia, se estima que entre 2020 y 2021 el número de usuarios se incrementó en 300 millones de personas, al pasar de 4,600 millones a 4,900 millones de personas (ITU, 2021b). También, se estima crezca en 1,000 millones de personas para 2025, esto detonó el incremento de gasto de los gobiernos

**DOI:** https://doi.org/10.22201/cisan.24487228e.2024.1.663
Versión *Ahead-of-Print*

vinculados a ciberseguridad. En este sentido, Mordor Intelligence (2021) externa que el mercado de ciberseguridad para los gobiernos, empresas privadas y usuarios de internet crecerá en un 378% en 2026.

Esta información es vital cuándo se aborda la región de América del Norte. Por ejemplo, Intersog (2022) indica que la región concentra el 40% de los ciberataques a nivel internacional. Y es la zona del planeta con el mayor nivel de incidencia de ataques y delitos cibernéticos del mundo, encima de Europa, Asía Pacífico, Sudamérica y África. También, prevé incrementará con el reciente auge de tecnologías como las redes 5G, la Inteligencia Artificial (IA) o el Computo Cuántico, que hacen más necesario que nunca el desarrollo de una política nacional y regional de ciberseguridad en Norteamérica.

**Gráfica 1. Número de ciberataques a nivel internacional por regiones (porcentaje).**




**Fuente: Intersog (2023).**

Sin embargo, existen múltiples disparidades entre México, Estados Unidos y Canadá para consolidar una política regional en la materia. Estas diferencias pueden asociarse al perfil y papel que tiene cada uno de los tres países como actor regional e internacional. También, al nivel de consolidación institucional y el proceso de creación de una política nacional de ciberseguridad que han recorrido de manera autónoma cada país. En ese sentido, la investigación parte de las siguientes dos hipótesis: 1) Estados Unidos y Canadá, al ser el primero una potencia global, y el segunda regional, detentan un perfil de naciones con una política exterior activa de impacto regional e internacional en ciberseguridad. 2) La

**DOI:** https://doi.org/10.22201/cisan.24487228e.2024.1.663
Versión *Ahead-of-Print*

trayectoria histórica individual de más de dos décadas, tanto de Estados Unidos como Canadá, explican el nivel de consolidación en el desarrollo de su política nacional de ciberseguridad frente a México.

Por esto, el artículo se divide en cinco secciones: 1) Discusión desde las teorías de relaciones internacionales, aplicada al contexto de la ciberseguridad, para identificar con base al realismo, liberalismo, constructivismo y la teoría de la guerra, qué tipo de perfil regional e internacional detentan cada uno de los tres países. 2) Un análisis de política internacional de los países de Norteamérica, a través de la revisión de métricas e índices internacionales que permitan ver el nivel de consolidación de capacidades cibernéticas, así como el papel que detentan en materia de ciberseguridad. 3) Análisis de política nacional de los tres países, a través de su marco institucional interno en materia de ciberseguridad, con la finalidad de identificar y explicar las disparidades existentes entre México con Estados Unidos y Canadá. 4) Por último, se presentan unas breves conclusiones.

Discusión de las teorías de relaciones internacionales a aplicadas a la ciberseguridad
Los estudios de ciberseguridad pueden servirse de las teorías de relaciones internacionales para generar un marco de análisis que permita identificar y evaluar el nivel de desarrollo y consolidación de la política nacional en la materia de un país. En esta sección se presenta una propuesta que parte del Estado-Nación, y cómo éste a través de su política nacional e internacional de ciberseguridad, puede consolidar su papel de nación líder o de vanguardia frente a otras. La revisión teórica contempla a los paradigmas realista, liberal, constructivista y la teoría de la guerra. También, el ejercicio sirve para identificar a los actores y dinámicas globales que interrelacionan en el campo de la ciberseguridad desde la óptica de la política internacional.

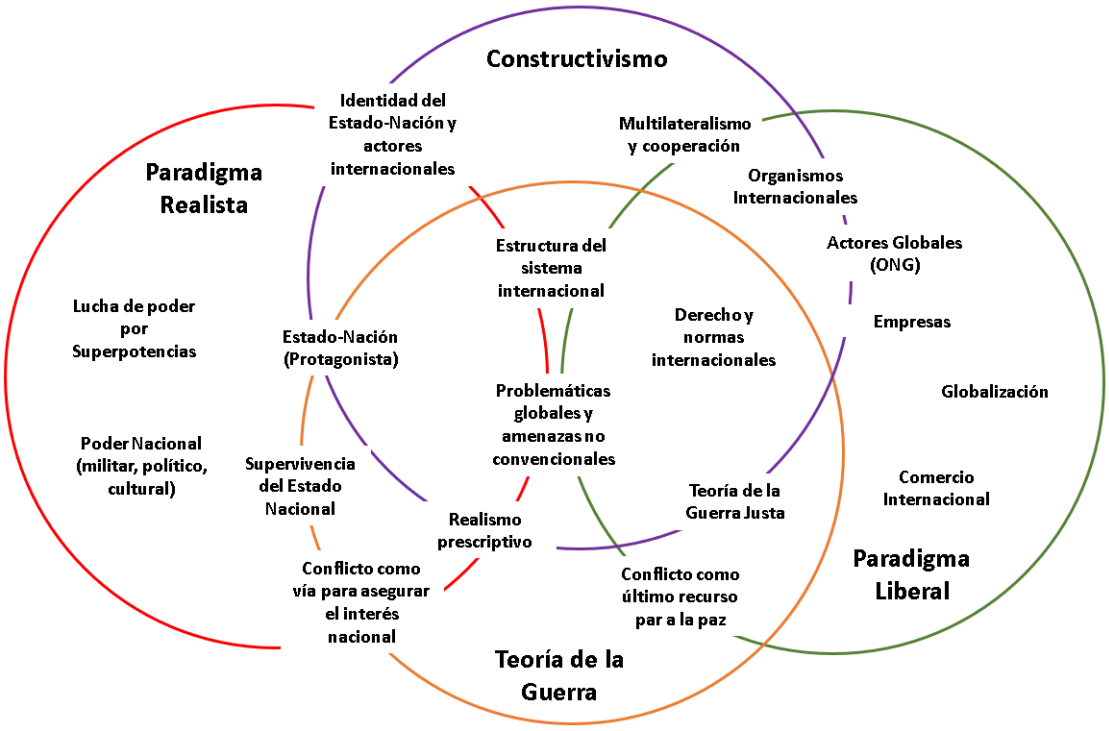
Es importante mencionar que esta propuesta es un ejercicio ecléctico que no se ajusta rígidamente a un paradigma de análisis o un conjunto de supuestos, sino que se basa en múltiples teorías, estilos e ideas para obtener amplios recursos para complementar a la ciberseguridad con las dinámicas de cooperación y conflicto que pueden existir entre las naciones. De esta forma, en la Figura 1 se presenta un modelo de análisis y abordaje teórico

**DOI:** https://doi.org/10.22201/cisan.24487228e.2024.1.663
Versión *Ahead-of-Print*

metodológico para las dinámicas de la política nacional e internacional de los Estados-Nación en materia de ciberseguridad, en el se presentan actores y dinámicas globales.

A continuación, se explica el enfoque y temas que aborda cada paradigma además que se sugieren algunas dinámicas que involucren a la ciberseguridad con la política nacional e internacional de los Estados-Nación, esta información es visible en la figura 1.

**Figura 1. Propuesta de modelo teórico-metodológico de análisis de la ciberseguridad para la política nacional e internacional desde las relaciones internacionales.**




**Fuente: Elaboración propia.**

***Paradigma realista***: este paradigma incluye elementos teóricos del realismo clásico y del neorrealismo. Dos conceptos clave de este esquema de pensamiento son la lucha por el poder en el sistema internacional y la existencia de la anarquía global. Ambas ideas se relacionan al término de ciber poder, categoría de análisis propuesta por Nye Jr. (2010) que externa que el ciberespacio es el quinto dominio del poder de los Estado-Nación para perseguir su interés nacional. También, el realismo se centra en calibrar el poder nacional

**DOI:** https://doi.org/10.22201/cisan.24487228e.2024.1.663
Versión *Ahead-of-Print*

de los países. Para esto es importante mencionar que existen métricas internacionales que abordan el tema del ciber poder, e incluso presentan propuestas para su medición, como el *National Cyber Power Index*[1] (NCPI), y el *Cyber Capabilities And National Power* (CCNP). En este paradigma el poder nacional de los Estados está estrechamente relacionado con categorías como el poder duro (*hard power*), entendido como la capacidad de influencia a través de la coerción que tiene un país por medio poderío militar, desde el realismo clásico. O desde factores como la influencia política, económica y cultural, según el neorrealismo (Nye Jr., 2024). Por último, el paradigma realista tiende puentes complementarios para el análisis ecléctico con el constructivismo y la teoría de la guerra, como se observa a manera de "Diagrama de Venn" en la figura 1. Estos paradigmas expresan que los conflictos suponen vías tangibles y aceptables para que las naciones alcancen su interés nacional y, en consecuencia, se superponen en algunas esferas con el paradigma realista.

***Constructivismo*:** este paradigma es un marco analítico que destaca por su propuesta de intersubjetividad para abordar fenómenos y sucesos internacionales. En él es importante el concepto de "identidad" presentado por Alexander Wendt que permite identificar y ahondar en los procesos históricos y contextuales que explican el papel, rol o dinámica que juegan los Estados-Nación, organismos internacionales, o incluso conflictos o dinámicas de paz en el sistema internacional (Wendt, 1999). Este paradigma ayuda a explicar por qué países como Rusia o Estados Unidos se asociación a roles de potencias bélicas, mientras que Suiza o Costa Rica detentan una tradición pacifista (Wendt, 2004). También, el constructivismo es útil para entender la identidad de organismos internacionales como la Organización de las Naciones Unidas (ONU), la Organización de los Estados Americanos (OEA) o la Unión Europea (UE), que si bien todos pueden son clasificados como instituciones supranacionales, distan de su naturaleza, funciones y reputación internacional (Finnemore, 1993). Asimismo, al hablar de procesos de paz y conflicto, el constructivismo propone utilizar elementos contextuales como las variables

1 Tanto una explicación del NCPI y del CCNP se presentan en la sección de metodología y materiales para la investigación de este artículo

**DOI:** https://doi.org/10.22201/cisan.24487228e.2024.1.663
Versión *Ahead-of-Print*

históricas, etnográficas, culturales y sociales para explicar las tensiones de países como Ucrania, Estonia y Georgia con Rusia, y como estas a su vez, son diferentes (Sürek, 2020).

Para el caso de la aplicación a la ciberseguridad, es importante mencionar que desde el 2007, y cómo consecuencia de un ciberataque DDoS ejecutado desde Rusia a Estonia, las naciones del mundo han desarrollado políticas nacionales de ciberseguridad que se ven reflejados en la construcción de Estrategias Nacionales de Ciberseguridad, legislaciones o acuerdos de cooperación internacional en la materia (Aguilar-Antonio, 2019). En ese sentido, el constructivismo es clave para ahondar en el perfil que tienen los países en este campo. Por ejemplo, no ejercen el mismo rol o tienen la misma reputación internacional países como Estados Unidos, Rusia, China o Reino Unido, que son considerados las potencias globales de ciberseguridad, a naciones con un perfil más cooperacionista como Estonia o Singapur (Wendt, 2004).

Asimismo, el constructivismo ayuda a explicar por qué una nación como Estonia en la actualidad es una potencia de la ciberseguridad, con potencial de frenar agresiones provenientes de Rusia, mientras Ucrania o Georgia no puede hacer frente a este adversario (Shackelford, 2009). Con lo cual el enfoque teórico ayuda a entender desde el concepto de "identidad" el rol o papel de un Estado-Nación en el sistema internacional, hasta los fines y objetivos de un tratado internacional, o las causas y determinantes socio históricas y culturales que explican un conflicto prolongado en el contexto global. Por último, se indica que este esquema tiene puntos de encuentro con el paradigma realista, liberal y la teoría de la guerra, con los cuales se complementa como instrumento reforzador de sus supuestos.

***Paradigma liberal:*** el liberalismo es un enfoque que presenta divergencias y antagonismos con el realismo, en la comprensión y análisis de la política internacional. Esto se da a razón de que promueve el multilateralismo y la cooperación, en la lógica de la diplomacia, y analiza el actuar de los Estados-Nación con base a normas y tratados cimentados en el derecho internacional para la construcción de la gobernanza global (Barnett y Finnemore, 2005). Esta visión es claramente contraria a la búsqueda de los intereses particulares y la condición de la anarquía global dentro de la comprensión realista.

**DOI:** https://doi.org/10.22201/cisan.24487228e.2024.1.663
Versión *Ahead-of-Print*

Por otra parte, es importante destacar que este paradigma juega un papel de trascendencia al abrir espacios a nuevos actores de las relaciones internacionales como las empresas trasnacionales, los organismos internacionales y Organizaciones No Gubernamentales (ONGs) (Moravcsik, 1992). También, fenómenos como la globalización y sus consecuencias en esferas como la economía y la cultura son unidades clave de análisis. En el caso de cuestiones de ciberseguridad se indica que hay organismos internacionales que promueven la gobernanza del ciberespacio como la Unión Internacional de Telecomunicaciones (UIT), a través del *Global Cybersecurity Index* (GCI) o países como Estonia que mantienen una política activa en la materia y promueven la construcción de capacidades cibernéticas con instrumentos como el *National Cybersecurity Index* (NCSI). Ambas medidas se centran en promover instrumentos que ayuden a las naciones a consolidar los requerimientos internacionales mínimos necesarios para la construcción de sus políticas nacionales o capacidades cibernéticas en ciberseguridad, y comprometerse con la gobernanza del ciberespacio (Keohane, 2012).

En este conjunto de acciones, también destacan iniciativas como el Convenio de Budapest (2001), formalmente conocido como el "Convenio sobre la Ciberdelincuencia", que es un tratado creado con el objetivo de combatir el ciberdelito y promover la cooperación internacional en asuntos relacionados con la delincuencia cibernética. El cuál es una iniciativa multilateral que pretende establecer un marco legal y una base para la cooperación internacional en la lucha contra el ciberdelito. O el Grupo de Expertos Gubernamentales sobre Ciberseguridad de las Naciones Unidas, que es una iniciativa multilateral que busca abordar los desafíos y riesgos de los países en el ciberespacio (Lewis, 2011).

**Teoría de la Guerra:** La teoría de la guerra tiene una interpenetración, al igual que el constructivismo, con los tres paradigmas anteriores. En primera instancia, respecto a su vinculación con el realismo, se empata con el núcleo más duro vinculado al realismo prescriptivo que se encarga de analizar la supervivencia del Estado-Nación como fin último y central del interés nacional, con lo cual se encarga de abordar los conflictos armados o guerras entre las naciones. En este cruce, se tejen puentes con el constructivismo, a razón

**DOI:** https://doi.org/10.22201/cisan.24487228e.2024.1.663
Versión *Ahead-of-Print*

de que es necesario identificar cómo se entiende y ve a sí mismo cada país a través de la construcción de su identidad y capacidades en la política internacional, para entrar o no en un conflicto armado. Y cómo un Estado-Nación utiliza todos los recursos que tiene a su disposición en los diferentes dominios (campo terrestre, marítimo, aéreo, espacial o el ciberespacio) para librar una guerra (Sylvester, 2012).

Por otra parte, el núcleo suave de la teoría de la guerra tiene una vertiente denominada "teoría de la guerra justa", está visión institucionalista se ajusta a los preceptos que están en el marco del derecho internacional humanitario para el análisis de los crímenes de guerra. Esta vertiente considera que las guerras entre los Estados-Nación sólo acontecen cuándo se han agotado todos los medios y los países entran en ellos cuándo quieren alcanzar un bien común, lo que en teoría se relaciona con una moral y ética imperante en el contexto global (Marín, 2005).

En la última década se ha visto el potencial de utilizar el ciberespacio en el marco de conflictos armados y no armados, así como en guerras entre países. Tales como el caso del uso de operaciones cibernéticas en la invasión de Abjasia y Osetia del Sur (2008) por parte de Rusia. O más recientemente en las incursiones de Amenazas Persistentes Avanzadas (APT) en la invasión de Ucrania a través de malwares como Industroyer 2.0 y Wiper. Frente a esto, surge la necesidad de clarificar y aplicar el derecho internacional humanitario en el marco de un conflicto. Uno de los esfuerzos más destacados en este sentido es el "Manual de Tallin sobre Derecho Internacional Aplicable a los Conflictos Cibernéticos", redactado por un grupo de expertos en el campo del derecho internacional y la seguridad cibernética, cuyo propósito es ofrecer orientación sobre la aplicación del derecho internacional a las operaciones cibernéticas en el contexto de un conflicto armado (Schmitt, 2013).

## Metodología y materiales para la investigación

La presente investigación tiene como estrategia metodología el utilizar un estudio comparativo de corte cualitativo. Este método es útil a razón que permite identificar y analizar similitudes y disimilitudes entre las unidades de estudio, en este caso los tres países de Norteamérica (Tonon, 2011). Sobre esto, Colino (2009) indica que este tipo de análisis

**DOI:** https://doi.org/10.22201/cisan.24487228e.2024.1.663
Versión *Ahead-of-Print*

es ágil en un número acotado de unidades de estudio, cómo lo son los socios de la región. Es importante indicar que el análisis comparativo se dividió en dos partes, el primero corresponde a analizar la política internacional y el papel global que detenta cada uno de los tres países en materia de ciberseguridad. Este análisis a su vez se subdivide en dos fases, en la primera se utiliza el GCI y el NCSI para contrastar el nivel de desarrollo de capacidades cibernéticas de Estados Unidos, Canadá y México e identificar las simetrías y asimetrías que existen entre los tres países. Estos dos índices se relacionan a una visión liberalista de la ciberseguridad, porque analizan el nivel de compromiso de los países con la cooperación multilateral y la construcción de la gobernanza del ciberespacio. De esta forma, es necesario explicar la estructurada cada métrica:

GCI: abocado a fomentar la cooperación internacional de las naciones, actores estatales y actores no estatales organizados, para garantizar la gobernanza y buena regulación del ciberespacio. El índice se divide en cinco pilares: 1) marco legal, 2) medidas técnicas, 3) estructura organizacional, 4) desarrollo de capacidades y 5) cooperación internacional. Ha tenido un total de cuatro iteraciones, realizadas en 2014, 2017, 2018 y 2020, hecho que permite ver la progresión y retrocesos de los países a lo largo del tiempo, es importante mencionar que evalúa a los 193 países del mundo (ITU, 2014; 2021a).

NCSI: la herramienta evalúa el desarrollo de capacidades cibernéticas de los Estados-Nación a través de 12 indicadores. Estos indicadores son: 1) desarrollo de política, 2) delimitación de amenazas, 3) desarrollo de educación, 4) aportación global, 5) nivel de desarrollo digital, 6) protección de servicios esenciales, 7) identificación electrónica y confidencialidad de servicios, 8) protección de datos personales, 9) respuesta a incidentes cibernéticos (CIRC), 10) administración de crisis cibernéticas, 11) política de lucha contra el cibercrimen y 12) operaciones militares. El NCSI se aplicó por primera vez en 2017 y proporciona información sobre 161 países. La herramienta es valiosa para evaluar la preparación de los países en materia de ciberseguridad e identificar áreas de mejora en sus estrategias y capacidades en la materia (E-Governance Academy, 2023).

Posteriormente, se presentan las métricas cercanas al paradigma realista, en este contexto, conceptos como la cooperación o el multilateralismo, son sustituidos por

términos como el ciber poder o capacidades efectivas para alcanzar intereses particulares en el quinto dominio. A continuación, se describen el NCPI y el CCNP:

NCPI: medida creada por el Belfer Center de la John F. Kennedy Government School de la Universidad de Harvard. Evalúa un total de 30 países en siete objetivos, en su edición de 2020, vinculados a la seguridad nacional y la política exterior, incluyendo 1) vigilancia y seguimiento de grupos domésticos, 2) fortalecimiento y mejora de la ciberdefensa nacional, 3) control y manipulación del entorno de información, 4) recopilación de inteligencia en otros países para la seguridad nacional, 5) creciente competencia comercial cibernética y tecnológica nacional, 6) destrucción o desactivación de la infraestructura y las capacidades de un adversario y 7) definición de normas técnicas y normas cibernéticas internacionales (Voo et al., 2020). Para su segunda edición en 2022, el NCPI anexó un nuevo indicador 8) acumular riqueza y/o extraer criptomonedas. El NCPI se ha realizado en dos ocasiones y es importante citar que resalta por su enfoque en las capacidades de defensa y ofensa de los países. La medida considera a Estados Unidos, China, Reino Unido, Rusia e Israel como potencias del ciberespacio. También, según su metodología, sólo evalúa a países del mundo que se asumen a sí mismos como potencias del ciberespacio (Voo et al., 2022).

El CCNP, publicado por el International Institute for Strategic Studies (IISS) es un estudio que proporciona una evaluación cualitativa de las capacidades cibernéticas de 15 países y un marco cualitativo para clasificar la capacidad cibernética estatal a nivel global. La metodología se centra en evaluar las capacidades cibernéticas de los estados y su contribución al poder nacional a través de factores como el ecosistema cibernético de cada, la competencia económica y los asuntos militares. También, destaca el contexto de creciente confrontación internacional en el ciberespacio, con ejemplos notables de declaraciones y acciones de potencias como China, Estados Unidos y Rusia (IISS, 2021). A las que subraya la importancia creciente de las políticas y capacidades cibernéticas en la seguridad internacional. El estudio ha sido publicado en dos ocasiones, la primera en 2021, en la que se analizaron a 15 países, mientras que el segundo, de 2023, se incluyeron naciones como Brasil, Estonia, Alemania, los Países Bajos, Nigeria, Arabia Saudita, Singapur, Sudáfrica, Turquía y los Emiratos Árabes Unidos, para alcanzar un total de 25 naciones. La

**DOI:** https://doi.org/10.22201/cisan.24487228e.2024.1.663
Versión *Ahead-of-Print*

evaluación se realiza en siete categorías: 1) estrategia y doctrina, 2) gobernanza, comando y control, 3) capacidad central de ciber inteligencia, 4) Empoderamiento y dependencia cibernéticos, 5) Seguridad y resiliencia cibernéticas, 6) liderazgo global en asuntos cibernéticos, 7) capacidad cibernética ofensiva. Por último, clasifica a los países en tres niveles de poder cibernético: 1) primer nivel para aquellos con fortalezas líderes en todas las categorías, 2) segundo nivel para aquellos con fortalezas líderes en algunas categorías y 3) tercer nivel para aquellos con fortalezas o potencial en algunas categorías, pero debilidades significativas en otras (IISS, 2023).

Con estos cuatro índices se identifica el papel que se otorga en el ámbito regional e internacional a cada uno de los tres países de América del Norte. También, el NCSI sirve para identificar sus áreas de convergencia y divergencia. Por lo cual realiza una revisión de fuentes abiertas gubernamentales, que permitieran describir y analizar la trayectoria de la política nacional de ciberseguridad de cada nación y hacer un comparativo en su nivel de consolidación de la construcción su política y capacidades cibernéticas.

## Análisis de política internacional de países de norteamérica

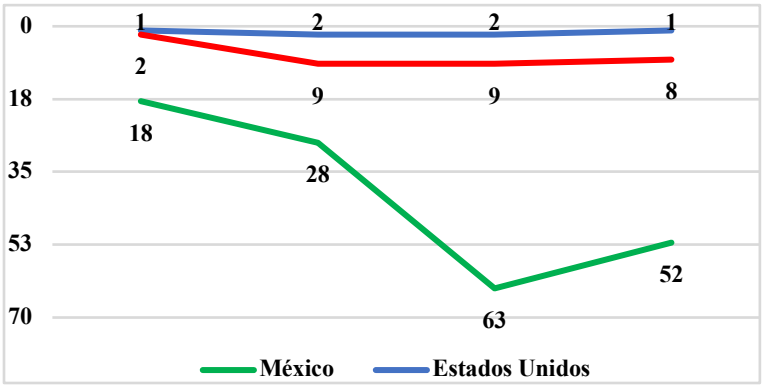
### Métricas cercanas al paradigma liberal

El continente americano, conformado por sus diferentes regiones como Norteamérica, Centroamérica y Sudamérica, se presenta como una de las zonas del planeta con las asimetrías más amplias en el desarrollo de capacidades y políticas nacionales de ciberseguridad. Alberga potencias globales y regionales, como Estados Unidos y Canadá, mientras que el resto de las naciones presentan un fuerte rezago. Con relación a América Latina, considerando la región desde México hasta Argentina, los países se encuentran en la sexta posición a nivel global, de un total de ocho regiones, en el desarrollo de capacidades cibernéticas, sólo delante de África y Oceanía (Aguilar-Antonio, 2020). Se considera que existen países que dan pasos estratégicos en la materia como Chile, Uruguay y Santa Lucía, países de desarrollo medio (México, Perú y Colombia) y países con un claro rezago internacional, Surinam, Trinidad y Tobago, etc. (Aguilar-Antonio, 2021).

**Norteamérica, Revista Académica del CISAN-UNAM, año 19, número 1, enero-junio de 2024**
**DOI:** https://doi.org/10.22201/cisan.24487228e.2024.1.663
Versión *Ahead-of-Print*

Esta situación es más evidente cuándo se analiza a las tres naciones de la región de Norteamérica, a través del GCI, dónde Estados Unidos alcanza una calificación de 100/100 puntos, Canadá ponderación de 97.6/100 y México una ponderación de 81.7/100, esto muestra un claro retraso de este último con sus dos socios regionales. Esta divergencia se ha vuelto más profunda en la última década, con base a los datos que presenta el GCI durante el periodo 2014-2021, porque Estados Unidos y Canadá se han mantenido a lo largo de los años como naciones de vanguardia en el desarrollo de su política de ciberseguridad, entre las primeras posiciones del índice. Mientras tanto, México mantiene un constante a rezago, donde es visible que esta brecha era menor en el año 2014, al ocupar este país la posición número 18, mientras Canadá y Estados Unidos estaban en la posición 1 y 2, respectivamente. Para el año 2021, México se encontró en la posición 52, mientras que el resto de los países de América del Norte se mantienen en los diez primeros puestos en el desarrollo de capacidades cibernéticas a nivel internacional como se observa en la gráfica 2.

**Gráfica 2. Progresión de países de América del Norte (Estados Unidos, México y Canadá) según en el GCI 2014-20212**




**Fuente: ITU (2014-2021a).**

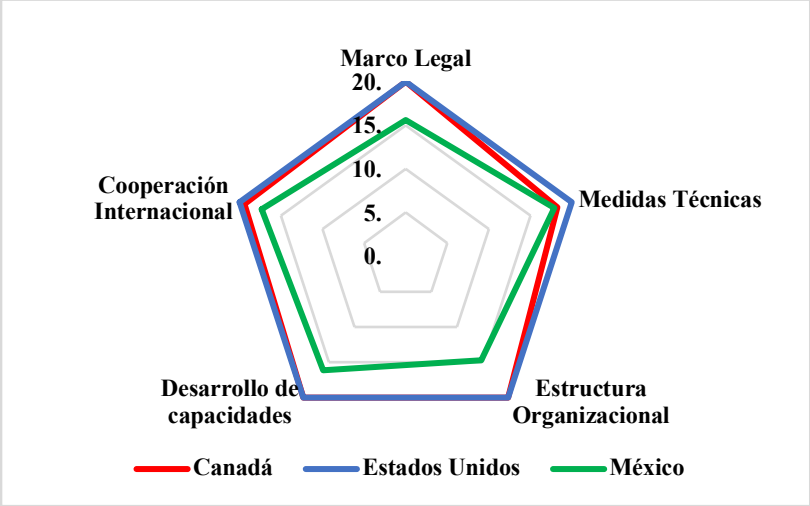
En el marco de la ponderación de las cinco dimensiones del GCI, México se presenta con claros rezagos en cada dimensión respecto a a Estados Unidos y Canadá. Por ejemplo,

2 El gráfico está en orden inverso a razón de que la posición número uno representa a los países con el desarrollo más alto en ciberseguridad, mientras que los más alejados del 1 indican un mayor nivel de rezago.

**Norteamérica, Revista Académica del CISAN-UNAM, año 19, número 1, enero-junio de 2024**
**DOI:** https://doi.org/10.22201/cisan.24487228e.2024.1.663
Versión *Ahead-of-Print*

para el caso de Estados Unidos, es importante mencionar que alcanza una calificación de 20/20 puntos en las cinco dimensiones, con lo cual se le considera una potencia del ciberespacio. Por su parte, Canadá alcanza la máxima ponderación en las dimensiones de marco legal (20/20), estructura organizacional (20/20) y desarrollo de capacidades (20/20). Mientras que en medidas técnicas alcanza un puntaje de 18.2/20 puntos y en cooperación internacional 19.4/20 puntos. Por último, México alcanza los siguientes puntajes en cada dimensión: 15.6/20 puntos en marco legal, 17.9/20 en medidas técnicas, 14.7/20 en estructura organizacional, 16.13/20 en desarrollo de capacidades y 17.3/20 en cooperación internacional. Con lo cual México detenta un claro rezago respecto a sus socios en la región en las cinco dimensiones. Eso implica que el país tiene un menor nivel de compromiso con documentos como son la Agenda Global de Ciberseguridad, de la ITU, creada en 2004, que tiene como fin promover el compromiso de los países con la cooperación y el multilateralismo para la gobernanza global de ciberespacio.

**Gráfica 3. Comparativo de naciones de América del Norte en el desarrollo de capacidades cibernéticas según las 5 dimensiones del GCI (2021)**



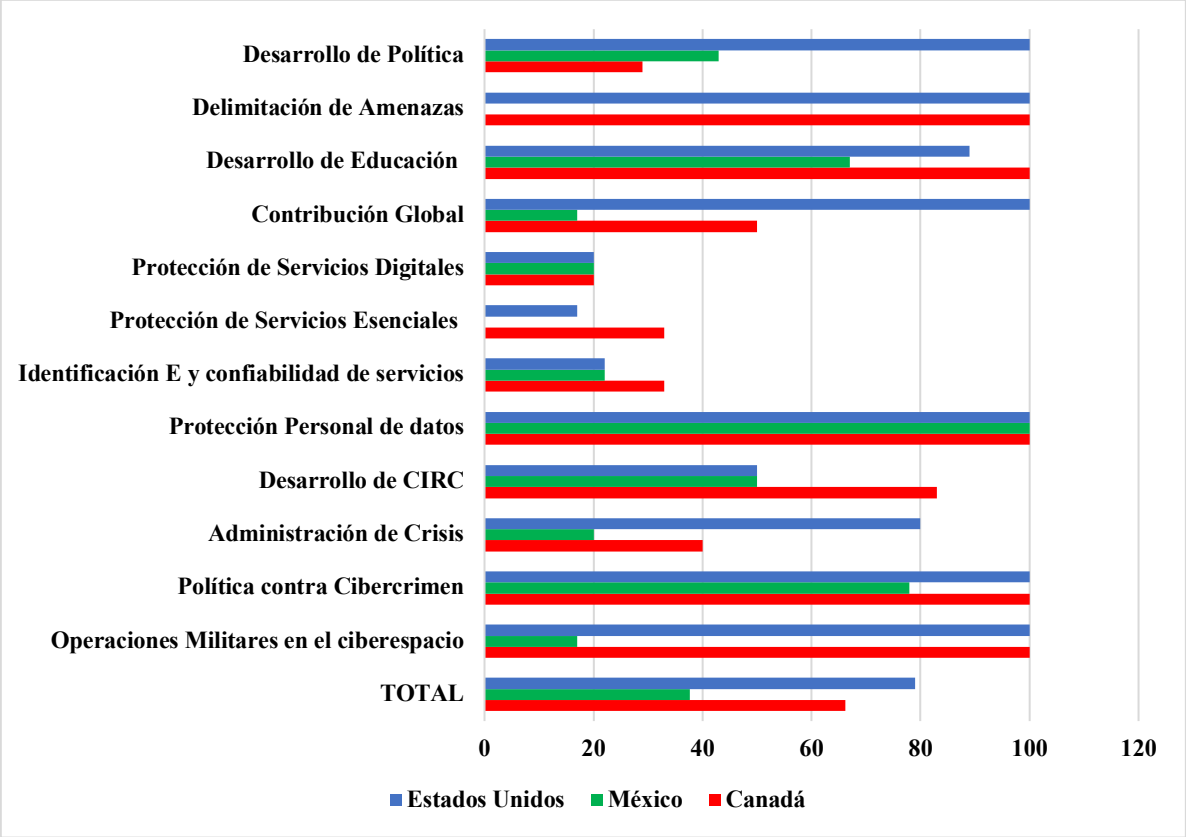

**Fuente: GCI (2021a).**

Respecto a la metodología del NCSI se presenta el panorama de que México presenta fuertes rezagos frente a Estados Unidos y Canadá en diez de doce dimensiones. Sólo en el indicador de política de protección de datos y protección de servicios digitales

**DOI:** https://doi.org/10.22201/cisan.24487228e.2024.1.663
Versión *Ahead-of-Print*

presentan ponderaciones semejantes. Sin embargo, el puntaje global del NCSI otorgan calificación de 79/100 puntos a Estados Unidos, 66.2/100 a Canadá y 37.7/100 a México.

**Gráfico 4. Comparativo de países de América del Norte en los indicadores del NCSI (2023).**




**Fuente: E-Governance Academy (2021).**

Esto presenta la condición de un fuerte rezago para México respecto a sus socios en América del Norte, dónde Estados Unidos es considerado un país líder global y Canadá un líder regional en materia de ciberseguridad. También, derivado de este análisis el NCSI resultó útil para identificar las dimensiones en las cuales el conjunto de países tiende a la simetría y la asimetría en sus políticas y capacidades cibernéticas. Por esta razón se crearon cuatro categorías de análisis para cada uno de los doce indicadores, los cuales son: 1. Simetría entre Estados Unidos, Canadá y México. 2. Simetría Estados Unidos-Canadá y rezago de México. 3. Liderazgo de Estados Unidos, y 4. Liderazgo de Canadá, visibles en la figura 2.

**Norteamérica, Revista Académica del CISAN-UNAM, año 19, número 1, enero-junio de 2024**
**DOI:** https://doi.org/10.22201/cisan.24487228e.2024.1.663
Versión *Ahead-of-Print*

**Figura 2. Categorías sobre el desarrollo capacidades cibernéticas de América del Norte.**

| Categoría | Indicadores | Ponderaciones | | |
|---|---|---|---|---|
| I. Simetría entre Estados Unidos, Canadá y México | Protección personal de datos | EUA 100 | Canadá 100 | México: 100 |
| | Protección de servicios digitales | 20 | 20 | 20 |
| II. Simetría Estados Unidos-Canadá y rezago de México | Operaciones militares en el ciberespacio | 100 | 100 | 17 |
| | Política contra cibercrimen | 100 | 100 | 78 |
| | Delimitación de amenazas | 100 | 100 | 0 |
| III. Liderazgo de Estados Unidos | Administración de Crisis | 80 | 40 | 20 |
| | Protección de Servicios Esenciales | 17 | 33 | 0 |
| | Contribución Global | 100 | 50 | 17 |
| | Desarrollo de Política | 100 | 29 | 43 |
| IV. Liderazgo de Canadá | Desarrollo de CIRC | 50 | 83 | 50 |
| | Identificación E y confiabilidad de servicios | 22 | 33 | 22 |
| | Desarrollo en educación | 89 | 100 | 67 |

**Fuente: Elaboración propia con base a E-Governance Academy (2023).**

## Métricas cercanas al paradigma realista

Cómo se mencionó en la subsección anterior, América del Norte es una región que cuenta con dos naciones consideradas líderes globales en materia de ciberseguridad. En el caso de

**DOI:** https://doi.org/10.22201/cisan.24487228e.2024.1.663
Versión *Ahead-of-Print*

los Estados Unidos, el país es la principal potencia económica y militar del mundo, en la actualidad, y está condición se traslada al ciberespacio como componente de su poder nacional. No es sorpresa observar que tanto métricas como el NCPI y el CCNP consideran al país la principal potencia del ciberespacio, con capacidades efectivas para alcanzar su interés nacional y realizar acciones de coerción en contra de adversarios como China, Rusia o Irán (IISS, 2021).

Por su parte, Canadá no está considerada dentro de las cinco principales potencias del ciberespacio, por parte del NCPI, pero se le considera una potencia de segundo nivel o regional en el dominio. Esta condición se traslada al hecho de que Canadá es la onceava potencia económica del mundo, según datos del Banco Mundial, está condición, le permite ocupar posiciones privilegiadas en organismos internacionales como el Banco Mundial, el G7 y el G20. En el ámbito regional, el país cuenta con un mejor prestigio que Estados Unidos y esto se refleja en sus iniciativas de cooperación en el continente en organismos como la OEA. También, a pesar de que el país no figura entre los diez ejércitos más poderosos del mundo, se considerada posee capacidades militares moderadas, las cuales se ven reflejadas en aspectos como su membresía en la Organización del Tratado del Atlántico Norte (OTAN). Asimismo, es considerado un aliado estratégico por su vecino del sur en el marco del NORAD (North American Aerospace Defense Command) y el Northcom (United States Northern Command) que contemplan al campo de la ciberseguridad (IISS, 2021).

Un aspecto que destaca del rezago de México en Norteamérica, desde la perspectiva realista, es el hecho de que tanto el NCPI, como el CCNP, no incluyen al país en su respectiva medición. Esto evidencia que México no se asume a sí mismo como una potencia del ciberespacio, lo que refleja que no tiene una política nacional bien estructurada en la materia. Tampoco, considera al dominio un campo de importancia para proyectar su interés nacional. Esta condición es una situación compartida con el resto de América Latina, con la excepción de Brasil, único país de América Latina considerado en las dos métricas citadas (Voo et al, 2021;2023, IISS, 2021;2023). Esto supone un problema a razón que no se puede comparar a México con sus vecinos del norte desde una perspectiva realista, a razón que ambas métricas no generan información sobre el país.

**DOI:** https://doi.org/10.22201/cisan.24487228e.2024.1.663
Versión *Ahead-of-Print*

A pesar de esta condición, se puede identificar el papel de potencia global de Estados Unidos, y de potencia media, o líder regional, de Canadá en ciberseguridad. Por ejemplo, destaca que en las dos iteracciones del NCPI, Estados Unidos estuvo en la primera posición rivalizando posición junto a China, Rusia o Reino Unido, considerados también potencias del ciberespacio. En el caso de Canadá, en la edición de 2020, el país estuvo en la posición número 8 de la nación con el ciber poder más completo de los 30 países. No obstante, para el 2022 fue desplazado hasta la posición 13, siendo sustituido por Vietnam. A pesar de esto, se le considera un país posee capacidades cibernéticas efectivas (Voo et al. 2023).

**Cuadro 1. Ranking de los 10 países con el ciber poder más completo según el NCPI 2020-2022.**

| Ranking | 2020 | 2022 |
|---|---|---|
| 1 | Estados Unidos | Estados Unidos |
| 2 | China | China |
| 3 | Reino Unido | Rusia |
| 4 | Rusia | Reino Unido |
| 5 | Países Bajos | Australia |
| 6 | Francia | Países Bajos |
| 7 | Alemania | Corea del Norte |
| 8 | Canadá | Vietnam |
| 9 | Japón | Francia |
| 10 | Australia | Irán |

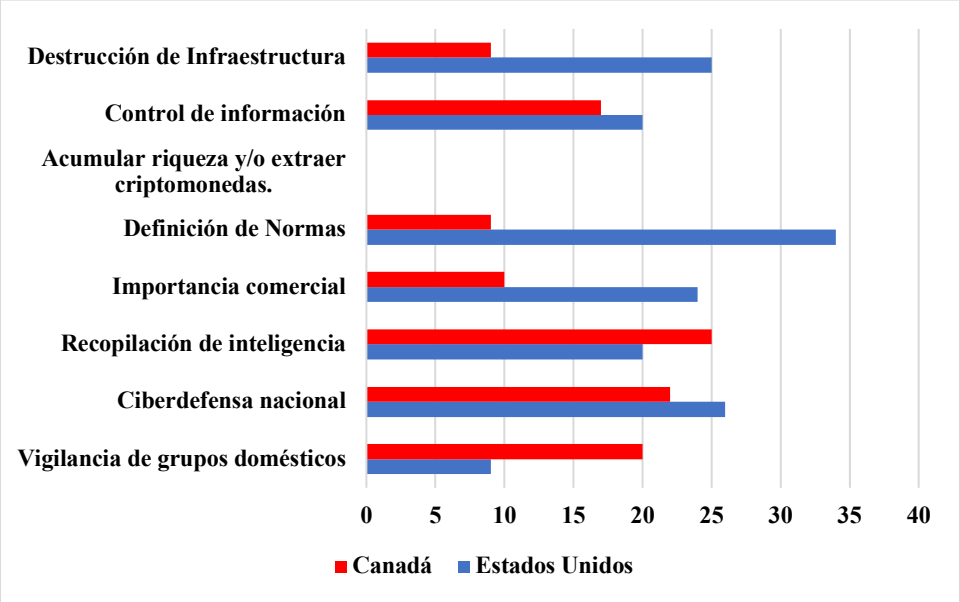
**Fuente: Voo et al., (2021;2023)**

Al hacer un comparativo entre los dos países, se encuentra que Estados Unidos supera a Canadá en cinco dimensiones: 1) fortalecimiento y mejora de la ciberdefensa nacional (26 puntos contra 22), 2) creciente competencia comercial cibernética y tecnológica nacional (24 contra 10), 3) definición de normas técnicas y normas cibernéticas internacionales (34 contra 9), 4) control y manipulación del entorno de información (20 contra 17), y 5) destrucción o desactivación de la infraestructura y las capacidades de un adversario (25 contra 9). Mientras que Canadá lidera en dos: 6) vigilancia y seguimiento de grupos domésticos (25 contra 9) y 7) recopilación de inteligencia en otros países para la

**DOI:** https://doi.org/10.22201/cisan.24487228e.2024.1.663
Versión *Ahead-of-Print*

seguridad nacional (25 contra 20). Por último, ambos países tienen una ponderación de 0 en la dimensión de 8) acumular riqueza y/o extraer criptomonedas.

**Gráfica 4. Comparativo de Estados Unidos y Canadá en el NCPI 2022.**




**Fuente: Voo et al. (2023).**

El CCNP abona información del papel de Estados Unidos como potencia global en ciberseguridad al presentar aspectos en los indicadores de estrategia, gobernanza, comando y control, capacidades cibernéticas, poder nacional, empoderamiento cibernético y dependencia. Por ejemplo, el estudio indica que, desde mediados de la década de 1990, el país ha buscado ser un actor líder en el quinto dominio. Y en la actualidad es el único país con una presencia global significativa tanto en el uso civil como militar del ciberespacio. A la par que percibe amenazas serias de China y Rusia, lo que lleva a un enfoque sólido y urgente para mejorar sus capacidades cibernéticas (IISS, 2021). También, cuenta con estrategias nacionales bien desarrolladas para la defensa y seguridad en el ciberespacio, centrándose en la defensa del territorio, conflictos de baja intensidad y guerra de alta

**DOI:** https://doi.org/10.22201/cisan.24487228e.2024.1.663
Versión *Ahead-of-Print*

intensidad. Por esto, Estados Unidos lidera la promoción de la gobernanza multisectorial en el ciberespacio, involucrando a diversas entidades como la comunidad de inteligencia, las fuerzas armadas y el sector privado en su política nacional. Esto ha consolidado capacidades de ciber inteligencia sofisticadas y extensas, lideradas por agencias como la NSA, CIA y FBI. A la par que colabora con extensamente con empresas del sector privado, universidades y socios internacionales, notablemente a través de la alianza Five Eyes (Pfluke, 2019).

También, el CCNP indica que el país es el más poderoso en términos de capacidad de Tecnologías de la Información y Comunicación (TIC). Y es líder en la economía digital global, con una participación significativa en plataformas digitales globales, inversión de capital de riesgo y gastos en investigación y desarrollo. Respecto a la capacidad de resiliencia cibernética frente a ciberataques, se indica que ha defendido activamente su infraestructura crítica de información desde la década de 1990, reconociendo la dificultad de la tarea. No obstante, se reconoce que ha sido objeto de vulneraciones exitosas, como fue la operación rusa de ciberespionaje a la empresa SolarWinds (Willett, 2023). Por lo que el gobierno está activamente involucrado en detectar y neutralizar amenazas en colaboración del sector privado.

Asimismo, desde el 2003, Estados Unidos lideró una iniciativa en el G8 que resultó en la adopción de 11 principios para proteger la infraestructura crítica, demostrando su compromiso con la cooperación internacional (Sussmann, 2017). Esto promovió la adopción de normas voluntarias para la ciberseguridad en 2015, a pesar de las crecientes tensiones con China y Rusia. A pesar de tener un enfoque cooperacionista, el país también cuenta con capacidades efectivas para hacer operaciones cibernéticas contra sus adversarios, por ejemplo, en 2008 la operación Stuxnet a la central nuclear de Natanz, en Irán afirman la capacidad ofensiva del país. También, desde 2015 realiza operaciones cibernéticas para neutralizar acciones de Estado islámico (ISIS) y la Agencia de Investigación de Internet de Rusia (Francois y Lin, 2021, Temple-Raston, 2021).

Respecto a Canadá, el CCNP indica que este país sigue un enfoque integral de toda la sociedad para la ciberseguridad, alineado con su sistema de gobierno y política exterior. En este sentido, el país tiene un enfoque de partes interesadas, con una capacidad

**DOI:** https://doi.org/10.22201/cisan.24487228e.2024.1.663
Versión *Ahead-of-Print*

cibernética en el sector civil madura, respaldada por leyes y regulaciones adecuadas. Con lo cual, sigue un enfoque multiactor para la política de ciberseguridad y colabora con varios organismos gubernamentales, incluidos el Communications Security Establishment (CSE) y el Canadian Security Intelligence Service (CSIS). Esto esquema se ve apoyado en el hecho de que el país tiene un sector tecnológico robusto, especialmente en áreas como inteligencia artificial (IA) y tecnología digital, siendo Toronto un centro importante (IISS, 2021). Para esto, los documentos clave centrados en la ciberseguridad incluyen estrategias realizadas en los años 2010 y 2018.

Respecto a sus capacidades cibernéticas ofensivas, el país estableció una fuerza cibernética en 2019. Sin embargo, las operaciones cibernéticas ofensivas requieren la aprobación gubernamental caso por caso, de manera consistente con el uso de otros activos militares. Respecto a su compromiso global, Canadá participa activamente en foros internacionales sobre asuntos cibernéticos, buscando dar forma al entorno internacional de ciberseguridad, tales como el Grupo de Expertos Gubernamentales de Naciones Unidas sobre seguridad en el ciberespacio. Y ha contribuido a la creación de capacidad de ciberseguridad a nivel global, dese la OEA, con esto reafirma su carácter de líder regional en el ciberespacio (IISS, 2021).

## Análisis de política nacional de países de norteamérica

La sección anterior se centró en analizar la política internacional de los tres países Norteamérica en materia de ciberseguridad. Esto mostró múltiples evidencias de los factores que posicionan a Estados Unidos, como una potencia global, y Canadá, como potencia regional la materia. También, la revisión del NCSI permitió identificar cuatro dimensiones del análisis que permiten identificar las diferencias que explican el rezago de México en el desarrollo de su política nacional y capacidades cibernéticas: 1. Simetría entre Estados Unidos, Canadá y México. 2. Simetría Estados Unidos-Canadá y rezago de México. 3. Liderazgo de Estados Unidos, y 4. Liderazgo de Canadá. Estas cuatro clasificaciones, suponen que sólo en la primera categoría el país se encuentra en equilibrio con sus socios

**DOI:** https://doi.org/10.22201/cisan.24487228e.2024.1.663
Versión *Ahead-of-Print*

regionales. Mientras que en el resto el país muestra clara rezagos frente a liderazgos de Canadá y Estados Unidos.

De esta forma, en el análisis de la política nacional de ciberseguridad se dividió en dos partes: 1) el primero en abordar desde el indicador de política de protección de datos, en el que existe simetría entre México y sus vecinos del Norte. 2) el análisis de los indicadores de desarrollo de política nacional, protección de servicios esenciales y política contra el cibercrimen, que evidencian el rezago de México en materia de ciberseguridad.

Simetría entre Estados Unidos, Canadá y México

Para analizar la política de protección de datos de los tres países se utilizaron los subindicadores de protección de datos según el NCSI para hacer un análisis comparativo. Por medio de una revisión de fuentes abiertas y gubernamentales se identificaron las legislaciones e instituciones que dan cumplimiento en la materia, esto se presenta en la figura 3. En el marco del análisis comparativo, se puede argumentar que, en el caso de Estados Unidos, como actor clave en el sistema internacional, este país ha adoptado una perspectiva descentralizada en su política de protección de datos. Las múltiples leyes federales y estatales abordan aspectos específicos de la privacidad y seguridad de los datos, reflejando la preferencia estadounidense por la autonomía individual y la limitación de la intervención gubernamental, posición cercana al paradigma liberal de las relaciones internacionales (Boyne, 2018).

Es importante señalar que el país no cuenta con una ley de privacidad de datos integral a nivel federal, pero su política se conecta indirectamente con varios instrumentos internacionales. Aunque no es parte del Reglamento General de Protección de Datos (GDPR) de la Unión Europea, la relación comercial con la UE ha llevado a cumplir ciertos compromisos. Como crear la iniciativa del Escudo de Privacidad UE-EE. UU. (EU-U.S. Privacy Shield), acuerdo bilateral para facilitar la transferencia de datos personales, aunque este fue invalidado en 2020 (Charlsey, 2022). También, Estados Unidos ha participado en discusiones sobre normas internacionales de privacidad, como se evidencia en su presencia en la Conferencia Internacional de Autoridades de Protección de Datos y Privacidad (ICDPPC).

**Norteamérica, Revista Académica del CISAN-UNAM, año 19, número 1, enero-junio de 2024**
**DOI:** https://doi.org/10.22201/cisan.24487228e.2024.1.663
Versión *Ahead-of-Print*

**Figura 3. Comparación de política nacional de protección de datos personales de los tres países.**

| Protección personal de datos | | | |
|---|---|---|---|
| **Subindicador** | **Estados Unidos** | **México** | **Canadá** |
| **Leyes de protección de datos** | **Ley principal:**<br>Privacy Act of 1974<br>**Leyes complementarias:**<br>Driver's Privacy Protection Act (DPPA)<br>Children's Online Privacy Protection Act (COPPA)<br>Video Privacy Protection Act (VPPA)<br>Cable Communications Policy Act (CCPA)<br>Gramm-Leach-Bliley Act (GLBA)<br>Fair Credit Reporting Act (FCRA),<br>Health Insurance Portability and Accountability Act (HIPAA)<br>Telephone Consumer Protection Act (TCPA)<br>Family Educational Rights and Privacy Act (FERPA) | **Ley principal:**<br>Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO)<br>**Ley complementaria:**<br>Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) | **Ley principal:**<br>Personal Information Protection and Electronic Documents Act (PIPEDA)<br>**Leyes complementarias:**<br>Health Information Protection Act (HIPA)<br>Personal Information Protection Act (PIPA) - Columbia Británica<br>Privacy Act (Loi sur la protection des renseignements personnels)- Quebec<br>Personal Information Protection Act (PIPA) – Quebec |
| **Instituciones encargadas de la protección de datos** | Federal Trade Commission (FTC)<br>Department of Health and Human Services (HHS)<br>Office of Information and Privacy | Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) | Office of the Privacy Commissioner of Canada (OPC) |

**DOI:** https://doi.org/10.22201/cisan.24487228e.2024.1.663
Versión *Ahead-of-Print*

**Fuente: Elaboración propia.**

Para el caso de Canadá, la adopción de la Ley de Protección de Información Personal y Documentos Electrónicos (PIPEDA) refleja una postura más centralizada. Esto puede interpretarse como un intento de Canadá de ejercer mayor control sobre sus políticas de datos, reduciendo su dependencia de estándares externos. La PIPEDA, aplicada tanto al sector público como al privado, representa un compromiso con la construcción de una identidad digital nacional. No obstante, la existencia de leyes provinciales adicionales indica la necesidad de equilibrar la cohesión nacional con el respeto a la autonomía regional (Swartz, 2017).

A pesar del enfoque centralizado, la política de protección de datos también se relaciona con instrumentos internacionales. El país es signatario del Convenio 108 del Consejo de Europa, que establece principios para la protección de datos a nivel global (Kuner, 2018). Además, como miembro de la Organización para la Cooperación y el Desarrollo Económico (OCDE) sigue las directrices de la OCDE sobre protección de la privacidad y transmisión transfronteriza de datos. También, el país se adhirió al GDPR para la transferencia de datos con la UE, demostrando su compromiso con los estándares internacionales.

Sobre el caso de México, destaca que el país adoptó un enfoque dual con la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) y la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP). Del mismo modo, si bien participa en foros internacionales, como la ICDPPC, mostrando su interés y colaboración en la definición de estándares globales de protección de datos (Mendoza-Enríquez, 2018). Sus compromisos no alcanzas acuerdos en materia bilateral o multilateral como lo hacen Estados Unidos y Canadá con organismos como la Unión Europea. De hecho, destaca que el país tampoco cuenta con un mecanismo de cooperación con sus socios de Norteamérica en materia de protección de datos, lo que denota que, a pesar de estar en equilibrio con sus socios en esta dimensión, el país tampoco tiene una política internacional activa en la materia. Aspecto que se asemeja a su poca consolidación de una política nacional de ciberseguridad.

**DOI:** https://doi.org/10.22201/cisan.24487228e.2024.1.663
Versión *Ahead-of-Print*

**Simetría o liderazgo de Estados Unidos o Canadá frente a rezago de México**

Para analizar el rezago de México frente a sus socios de América del Norte se utilizaron tres indicadores de NCSI: 1) desarrollo de política nacional de ciberseguridad, 2) protección de servicios esenciales y 3) política contra cibercrimen. En consecuencia, se procedió a buscar los elementos que cumplan los subindicadores en fuentes abiertas, gubernamentales e institucionales de los tres países, el resultado se presenta en la figura 4.

El análisis del indicador de desarrollo de política nacional destaca la trayectoria de Estados Unidos como pionero en la región de Norteamérica, ya que la evolución de su política de ciberseguridad se remonta a principios de la década de 2000 (Roesener, Bottolfson y Fernandez, 2014). Durante el mandato del presidente Barack Obama se promulgó la "National Cybersecurity Protection Act" marcando el inicio de un enfoque integral. También, la creación del "Cybersecurity National Action Plan" y el "Department of Defense Cyber Strategy" durante su segundo mandato demostró el compromiso continuo en el fortalecimiento de la ciberseguridad. Para la administración de Donald Trump, el gobierno se centró en áreas específicas como las redes 5G, dando lugar a la "National Strategy to Secure 5G of the United States of America" (Gagnon y Rapin, 2021). Y la continuidad bajo la administración de Joe Biden se refleja en la creación de la "National Cybersecurity Strategy" consolidando un enfoque a largo plazo. El país ha liderado la formulación de políticas de ciberseguridad con un enfoque integral. La creación de la "Cybersecurity and Infrastructure Security Agency (CISA)" y el "Bureau of Cyberspace and Digital Policy" demuestra un compromiso sólido que evoluciona a lo largo de las administraciones y refleja una adaptación continua a las cambiantes amenazas digitales.

En el caso de Canadá, el país adopta una postura proactiva desde 2009 con el "Action Plan 2010-2015 for Canada's Cyber Security Strategy", esta estrategia se actualiza en 2018 con la "National Cyber Security Strategy". Y se consolida con el "National Cyber Security Action Plan (2019-2024)", que coordina la implementación de políticas de ciberseguridad. Por su parte, ha establecido como instituciones eje el "Canadian Centre for Cyber Security", agencia gubernamental dedicada exclusivamente a liderar y coordinar los esfuerzos de ciberseguridad frente a las amenazas cibernéticas.

**DOI:** https://doi.org/10.22201/cisan.24487228e.2024.1.663
Versión *Ahead-of-Print*

Para el caso de México, este inicia su incursión en políticas de ciberseguridad en 2017 con la publicación de la "Estrategia Nacional de Ciberseguridad" (Aguilar-Antonio, 2019, Quezada Aguirre, 2021). Sin embargo, este documento nunca llegó a implementarse y su existencia quedó en el olvido durante la transición de gobiernos de Enrique Peña Nieto a Andrés Manuel López Obrador (Aguilar-Antonio, 2020). La falta de una entidad claramente designada y de coordinación a nivel nacional plantea interrogantes sobre la efectividad de las políticas mexicanas en ciberseguridad

Respecto a la política de protección de servicios esenciales, se destaca que en Estados Unidos tiene sus raíces en la administración de Barack Obama, con la emisión de la "Policy Directive -- Critical Infrastructure Security and Resilience (PPD-21)", en 2013 (Lewis, 2019). Esta directiva estableció la política y directrices federales para fortalecer y proteger las infraestructuras críticas del país contra amenazas cibernéticas y físicas. Asimismo, a lo largo de las administraciones de Trump y Biden, se han emitido órdenes ejecutivas y directivas adicionales, destacando la atención continua a la ciberseguridad de las infraestructuras críticas. La "Cybersecurity and Infrastructure Security Agency" (CISA) se ha destacado como la agencia responsable en ciberseguridad e infraestructuras críticas en Estados Unidos. Establecida por la "Cybersecurity and Infrastructure Security Agency Act of 2018" desempeña un papel fundamental en la gestión de riesgos cibernéticos y la protección de infraestructuras críticas. También, es importante mencionar que su clasificación de las infraestructuras de Estados Unidos en 16 sectores[3], es una de la más completa a nivel mundial (CISA) (Humphreys, 2019).

Por su parte, Canadá inició su política de protección de infraestructuras esenciales en 2009 con la "National Strategy for Critical Infrastructure". A lo largo de los años, se ha fortalecido mediante documentos adicionales y la colaboración activa entre gobiernos y

3 Estos sectores incluyen: 1. energía, 2. agua y aguas residuales, 3. tecnologías de la información y comunicaciones, 4. instalaciones de fabricación, 5. transporte, 6. servicios de emergencia, 7. salud pública, 8. alimentación y agricultura, 9. servicios financieros, 10. gobierno, 11. instalaciones nucleares, 12. defensa industrial base, 13. comercio, 14. comunicaciones, 15. agencias de seguridad nacional y 16. funciones críticas de fabricación. Cada uno de estos sectores desempeña un papel crucial en la sociedad y la economía, y la CISA trabaja para fortalecer la seguridad cibernética y la resiliencia en cada uno de ellos.

**DOI:** https://doi.org/10.22201/cisan.24487228e.2024.1.663
Versión *Ahead-of-Print*

operadores a través de iniciativas como el "National Cross Sector Forum Action Plan for Critical Infrastructure". Aunque carece de legislación específica para la gestión de riesgos cibernéticos por parte de los operadores, se aborda dentro de la colaboración intersectorial.

También, el "Department of Public Safety Canada" se identifica como la autoridad competente en ciberseguridad y seguridad de la información en Canadá. Esta institución identifica 10 sectores[4] clave de infraestructura crítica (Public Safety, 2023). Y, aunque no hay legislación específica para la gestión de riesgos cibernéticos por parte de los operadores, el Foro Nacional Intersectorial Plan de Acción para Infraestructura Crítica aborda estas preocupaciones.

En México, las primeras nociones de protección de infraestructuras críticas se remontan a la "Ley de Seguridad Nacional" de 2006. Sin embargo, la conexión específica con la ciberseguridad no está claramente establecida en esta legislación. Documentos como la "Guía de Ciberseguridad para Instalaciones Públicas de México" y el "Protocolo Nacional Homologado de Gestión de Incidentes Cibernéticos" han contribuido a la conciencia en la materia (Gobierno de México, 2018;2023). Sobre este último documento, resalta que la Guardia Nacional identifica 16 sectores de infraestructuras esenciales, justificando está clasificación en el marco NIST, sin embargo, estos son los mismos sectores que presenta la CISA, en Estados Unidos, lo que pareció influenciar la delimitación. No obstante, la falta de énfasis en ciberseguridad en el "Programa Nacional de Infraestructura de la Calidad 2023" señala áreas de mejora. Esto se refleja que en no hay una autoridad competente para la protección de infraestructuras, lo que es consecuencia de la falta de legislación específica para la gestión de riesgos cibernéticos y la supervisión de operadores de servicios esenciales.

En el caso del indicador de política contra el cibercrimen, el análisis destaca que Estados Unidos cuenta con un marco legal extenso que ha evolucionado desde la "Computer Fraud and Abuse Act", de 1986, hasta leyes más recientes como la

4 Los sectores son: 1. Energía y Servicios Públicos, 2. Finanzas, 3. Alimentación, 4. Transporte, 5. Gobierno, 6. Tecnologías de la Información y Comunicación, 7. Salud, 8. Agua, 9. Seguridad y 10. Manufactura.

**DOI:** https://doi.org/10.22201/cisan.24487228e.2024.1.663
Versión *Ahead-of-Print*

"Cybersecurity Information Sharing Act", de 2015. Asimismo, cuenta con agencias y grupos de trabajo que hacen efectiva a la política como la "National Cyber Investigative Joint Task Force (NCIJTF)" y el "Cyber Forensics Working Group (CFWG)" que son iniciativas gubernamentales que involucran a diversas agencias para combatir la ciberdelincuencia.

El éxito de marco del marco legal e institucional puede observarse en documentos como el "Report Of The Attorney General's Cyber Digital Task Force" publicado por el "Deparment of Justice", en 2018. En él se documentan múltiples casos de combate a los delitos cibernéticos que han realizado instituciones como el FBI, la CIA y la Fiscalía Federal. En lo particular, este documento comparte casos de éxito como la neutralización de redes bots de casos como representativos como VPNFilter, Kelihos, Avalanche y Corefood, que estaban involucrados con robo de datos que derivó en pérdidas millonarias para gobiernos, empresas y usuarios. También, se resalta la capacidad de combate a mercados criminales en línea que operan en la Dark Web, como es el caso de AlphaBay y Hansa, Silk Road y Darkode. En los cuáles los instrumentos de cooperación internacional de Estados Unidos ayudaron a la captura y sentencia de delincuentes criminales (U.S Department of Justice, 2018).

En el caso de Canadá las principales leyes y regulaciones son la "Protecting Canadians from Online Crime Act" y la "Personal Information Protection and Electronic Documents Act". Mientras que las agencias y unidades centrales son la "Royal Canadian Mounted Police (RCMP)", que es la institución principal para combatir la delincuencia cibernética, y su unidad de criminalística digital que es la "Technical Investigation Services (TIS)". De forma semejante a Estados Unidos, Canadá publica reporte de acceso público en los que muestra evidencia del éxito de sus operaciones cibernéticas, tal es el caso del "Royal Canadian Mounted Police 2022-23 Departmental Results Report". En este documento se presentan casos como el desmantelamiento de la infraestructura del grupo de *ransomware* HIVE, que se había dirigido a más de 1,500 víctimas en más de 80 países, por parte de la RCMP. Así como el desmantelamiento del grupo HIVE que administrativa el portal ílicito de la Dark Web denominado "Canadian HeadQuarters", el cuál tenía presencia internacional (RCMP, 2023).

**DOI:** https://doi.org/10.22201/cisan.24487228e.2024.1.663
Versión *Ahead-of-Print*

Por su parte, México ha establecido tipificaciones específicas para delitos informáticos en su Código Penal Federal, abordando temas como acceso ilegal, interceptación de datos, daños a sistemas informáticos, fraude informático, pornografía infantil en línea, hostigamiento cibernético, robo de identidad, etc. Mientras que sus principales agencias son la Unidad de Investigaciones Cibernéticas y Operaciones Tecnológicas de la Fiscalía General de la República (FGR) que lidera la lucha contra la ciberdelincuencia a nivel nacional. La Dirección General Científica de la Guardia Nacional es responsable de la criminalística digital. También, destaca la Dirección General de Asuntos Policiales Internacionales e Interpol de la FGR, que es el punto de contacto para el cibercrimen internacional.

Un aspecto central que parece consolidar la política contra cibercrimen tanto de Canadá como de Estados Unidos es su adhesión a instrumentos internacionales. Esto se refleja en el hecho de que ambos son miembros del Convenio de Budapest, al que Estados Unidos se sumó en 20006, y Canadá, en 2015. También, es importante mencionar que Canadá forma parte de la alianza de inteligencia "Five Eyes" junto con Estados Unidos, Reino Unido, Australia y Nueva Zelanda. Este, aunque no es un tratado formal es un grupo que colabora estrechamente en asuntos de inteligencia y seguridad cibernética, compartiendo información y recursos para abordar amenazas cibernéticas a nivel global. En el caso de Estados Unidos, el país es parte del Tratado de Asistencia Legal Mutua (MLAT) con lo cual tiene acuerdos MLAT con varios países, que incluyen disposiciones para la cooperación en investigaciones relacionadas con delitos cibernéticos. Estos tratados permiten compartir información y pruebas de manera legalmente vinculante. En este sentido, es importante mencionar que México no cuenta con ningún mecanismo de colaboración internacional de esta naturaleza.

**Norteamérica, Revista Académica del CISAN-UNAM, año 19, número 1, enero-junio de 2024**
**DOI:** https://doi.org/10.22201/cisan.24487228e.2024.1.663
Versión *Ahead-of-Print*

Figura 4. Comparación de política contra cibercrimen, política nacional de ciberseguridad y protección de servicios esenciales de los tres países.

**Desarrollo de Política Nacional de Ciberseguridad**

| Subindicador | Estados Unidos | México | Canadá |
|---|---|---|---|
| **Unidad de Políticas de Seguridad Cibernética** | Bureau of Cyberspace and Digital Policy del US Deparment of State<br><br>Cybersecurity and Infrastructure Security Agency (CISA) que forma parte de la estructura del US Deparment of Homeland Security | El país no cumple con el subindicador | Public Safety Canada<br><br>Canadian Centre for Cyber Security |
| **Coordinación de políticas de ciberseguridad** | Office of the Coordinator for Cyber Issues<br><br>Cybersecurity and Infrastructure Security Agency (CISA) | El país no cumple con el subindicador | El país no cumple con el subindicador |
| **Estrategia de seguridad cibernética** | Cybersecurity Enhancement Act (2014)<br><br>National Cybersecurity Protection Act of (2014)<br><br>Department of Defense Cyber Strategy (2018)<br>National Cyber Strategy (2018)<br>US Department of Homeland Security Cybersecurity Strategy (2018)<br>Department of State International Cyberspace Policy Strategy (2020)<br>National Strategy to Secure 5G of the United States of America (2020)<br><br>National Cybersecurity Strategy (2023)<br><br>National Cyber Workforce and Education Strategy (2023)<br><br>CISA Cybersecurity Strategic Plan 2024-2026 (2023) | Estrategia Nacional de Ciberseguridad (2017) | Action Plan 2010-2015 for Canada's Cyber Security Strategy<br><br>National Cyber Security Strategy (2018) |
| **Plan para implementar la estrategia de ciberseguridad** | Cybersecurity National Action Plan (2016)<br><br>Cybersecurity and Infrastructure Security Agency: Strategic Intent (2019)<br><br>National Cybersecurity Strategy Implementation Plan (2023) | El país no cumple con el subindicador | |

**Protección de servicios esenciales**

| Subindicador | Estados Unidos | México | Canadá |
|---|---|---|---|
| **Se identifican operadores de servicios esenciales** | **Administración de Barack Obama**<br><br>Policy Directive – Critical Infrastructure Security and Resilience<br><br>Administración de Donald Trump<br><br>Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure<br><br>Cybersecurity and Infrastructure Security Agency Act of 2018<br><br>Administración de Joe Biden<br><br>Proclamation on Critical Infrastructure Security and Resilience Month<br><br>National Cybersecurity Strategy | Guía de Ciberseguridad para Instalaciones Públicas de México (2018)<br><br>Protocolo Nacional Homologado de Gestión de Incidentes Cibernéticos (2023) | National Strategy for Critical Infrastructure<br><br>Fundamentals of Cyber Security for Canada's CI Community<br><br>Cross Sector Forum Action Plan for Critical Infrastructure 2018-2020 y 2020-2022 |
| **Requisitos de ciberseguridad para operadores de servicios esenciales** | Cybersecurity and Infrastructure Security Agency Act of 2018 | El país no cumple con el subindicador | Fundamentals of Cyber Security for Canada's CI Community<br><br>Cross Sector Forum Action Plan for Critical Infrastructure 2018-2020 y 2020-2022 |
| **Autoridad de control competente** | Cybersecurity and Infrastructure Security Agency (CISA) | El país no cumple con el subindicador | Department of Public Safety Canada |
| **Regula el seguimiento de las medidas de seguridad** | El país no cumple con el subindicador | El país no cumple con el subindicador | El país no cumple con el subindicador |

**Política contra el cibercrimen**

| Subindicador | Estados Unidos | México | Canadá |
|---|---|---|---|
| **Los ciberdelitos están tipificados** | Computer Fraud and Abuse Act (CFAA)<br>Communications Privacy Act (ECPA)<br><br>Controlling the Assault of Non-Solicited Pornography And Marketing (Act CAN-SPAM)<br><br>Critical Infrastructure Protection and Resilience Cybersecurity Act (CIPRA)<br><br>Cybersecurity Information Sharing Act (CISA) | Art. 210 Ter, Código Penal Federal<br><br>Art 211 bis 1, Código Penal Federal<br><br>Art 212 bis 1, Código Penal Federal<br><br>Artículo 223 Bis, Código Penal Federal<br><br>Art. 224 Bis, Código Penal Federal<br><br>Art. 259 Ter, Código Penal Federal | Personal Information Protection and Electronic Documents Act (PIPEDA)<br><br>Protecting Canadians from Online Crime Act |
| **Unidad de ciberdelincuencia** | National Cyber Investigative Joint Task Force (NCIJTF) | Unidad de Investigaciones Cibernéticas y Operaciones Tecnológicas de la Fiscalía General de la República (FGR) | Royal Canadian Mounted Police, Integrated Technological Crime Units (ITCUs) |
| **Unidad de criminalística digital** | Cyber Forensics Working Group (CFWG) | Dirección General Científica de la Guardia Nacional (GN) | Royal Canadian Mounted Police, Technical Investigation Services (TIS) |
| **Punto de contacto 24/7 para cibercrimen internacional** | Computer Crime and Intellectual Property Section (CCIPS) del U.S. Department of Justice | Unidad de Interpol de la Fiscalía General de la República (FGR) | Royal Canadian Mounted Police, National Operations Centre (NOC) |

**Fuente: Elaboración propia.**

.

**Norteamérica, Revista Académica del CISAN-UNAM, año 19, número 1, enero-junio de 2024**
**DOI:** https://doi.org/10.22201/cisan.24487228e.2024.1.637
**FR:** 25/10/2023
**FA:** 21/12/2023
Versión *Ahead-of-Print*

## Conclusiones

La presente investigación partió de las siguientes dos hipótesis: 1) Estados Unidos y Canadá, al ser el primero una potencia global, y el segunda regional, detentan un perfil de naciones con una política exterior activa de impacto regional e internacional en ciberseguridad. 2) La trayectoria histórica individual de más de dos décadas, tanto de Estados Unidos como Canadá, explican el nivel de consolidación en el desarrollo de su política nacional de ciberseguridad frente a México.

Una vez realizado el análisis dentro del marco de esta investigación, se puede externar que ambas hipótesis se verificaron a través del análisis de la política nacional e internacional en materia de ciberseguridad de los países. En atención a la revisión teórico, destaca que, en el caso del perfil tanto de Estados Unidos, como de Canadá, ambos países utilizan una política exterior que puede servirse de múltiples mecanismos para entender el enfoque que buscan estas naciones a través de diferentes foros o acciones internacionales. De esta forma, paradigmas tan antagónicos como el liberalismo y el realismo pueden utilizarse para analizar diferentes dimensiones de las políticas de ciberseguridad de estos países.

En este sentido, destacó la utilidad de los índices internacionales, con independencia de su cercanía a determinado paradigma teórico. Ya que, desde la visión realista, o liberal, Canadá y Estados Unidos cuentan con acciones, instituciones o políticas que permiten identificar el activismo de su política exterior en materia de ciberseguridad. En ese sentido, al pasar al análisis de políticas nacionales a través de los indicadores del NCSI, se identificó cómo estás subdimensiones de la creación de una política de ciberseguridad, como es el caso de la protección de datos, combate al cibercrimen o protección de infraestructuras, los dos países las vinculan con instrumentos internacionales que refuerzan sus capacidades cibernéticas en cada materia.

Por último, es importante destacar que la trayectoria histórica de las políticas de ciberseguridad de los socios de México tiene más de veinte años. Con lo cual, múltiples acciones gubernamentales, políticas de estado y convenios nacionales e internacionales, se han construido para fortalecer la ciberseguridad en Estados Unidos y Canadá. Si tuviéramos referirnos a la Estrategia Nacional de Ciberseguridad, de 2017, México sólo tiene una trayectoria de siete años,

en el que construcción e implementación de la política de ciberseguridad no se ha materializado. Frente a eso, se prevén fuerte disparidades por el rezago y las asimetría que posee México frente a las condiciones de líder global y regional de sus dos socios en Norteamérica. Lo cual será una problemática tanto en el ámbito del intercambio económico a través del T-MEC, como de las otras dimensiones holísticas que implica la ciberseguridad.

## Fuentes

Aguilar-Antonio, Juan Manuel

2019 Hechos ciberfísicos: una propuesta de análisis para ciberamenazas en las Estrategias Nacionales de Ciberseguridad. URVIO Revista Latinoamericana de Estudios de Seguridad, (25), 24-40. DOI: https://doi.org/10.17141/urvio.25.2019.4007

2020 Presente y futuro de los retos de la ciberseguridad en México, una propuesta para la seguridad nacional. Revista legislativa de estudios sociales y de opinión pública, 13(29), 83-120.

2020 "La brecha de ciberseguridad en América Latina frente al contexto global de cibera menazas", Revista de Estudios en Seguridad Internacional, 6(2), pp. 17-43. DOI: http://dx.doi.org/10.18847/1.12.2

2021 "Retos y oportunidades en materia de ciberseguridad de América Latina frente al contexto global de ciberamenazas a la seguridad nacional y política exterior". Estudios internacionales (Santiago), 53(198), 169-197. DOI: http://dx.doi.org/10.5354/0719-3769.2021.57067

Aguirre Quezada, Juan Pablo

2022 Ciberseguridad, desafío para México y trabajo legislativo. Cuaderno de Investigación No. 87 (Marzo 2022). Instituto Belisario Dominguez, en < https://bibliodigitalibd.senado.gob.mx/handle/123456789/5551?show=full>, consultada el 15 de enero de 2024.

Barnett, Michael & Finnemore, Martha

2005 The power of liberal international organizations. Power in global governance, 161, 163-171.

Boyne, Shawn

2018 Data protection in the United States. The American Journal of Comparative Law, 66(suppl_1), 299-343. DOI: https://doi.org/10.1093/ajcl/avy016

Charlsey, Kelly

2022 Data Privacy Regulations in the United States, China, and the European Union.

Colino, César

2009 Método comparativo. Diccionario Crítico de Ciencias Sociales. Terminología Científico-Social. Madrid-México: Plaza y Valdés.

Francois, Camille y Lin, Herb

2021 The strategic surprise of Russian information operations on social media in 2016 in the United States: mapping a blind spot. Journal of Cyber Policy, 6(1), 9-30.

International Institute for Strategic Studies (IISS)

2021 "Cyber Capabilities And National Power: A net Assesment", junio, en < https://www.iiss.org/research-paper//2021/06/cyber-capabilities-national-power>, consultada el 15 de enero de 2024.

2023 "Cyber Capabilities and National Power Volume 2", septiembre, en https://www.iiss.org/research-paper/2023/09/cyber-capabilities-national-power-volume-2/, consultada el 15 de enero de 2024.

E-Governance Academy

2023 "National Cyber Security Index", E-Governance Academy, en <https://ega.ee/project/national-cyber-security-index/>, consultada el 15 de enero de 2024.

Finnemore, Martha

1993 International organizations as teachers of norms: the United Nations Educational, Scientific, and Cutural Organization and science policy. International organization, 47(4), 565-597.

Gobierno de México

2018 "Guía de Ciberseguridad para Instalaciones Públicas de México", en < https://www.gob.mx/wikiguias/articulos/guia-de-ciberseguridad-para-instalaciones-publicas?idiom=es>, consultada el 15 de enero de 2024.

2023 "Protocolo Nacional Homologado de Gestión de Incidentes Cibernéticos", en < https://www.gob.mx/gncertmx/articulos/protocolo-283239>, consultada el 15 de enero de 2024.

Humphreys, Brian

2019 Critical infrastructure: emerging trends and policy considerations for congress. R45809. Congressional Research Service, Washington, DC.

Gagnon, Frédérick y Rapin, Alexis

2021 Cybersecurity in America: The US National Security Apparatus and Cyber Conflict Management. Conflicts, Crimes and Regulations in Cyberspace, 2, 43-62.

International Telecommunication Union (ITU)

2014 Global Cybersecurity Index, en <https://www.itu.int/pub/D-STR-SECU-2015>, consultada el 15 de enero de 2024.

2017 Global Cybersecurity Index, en <https://www.itu.int/pub/D-STR-GCI.01-2017>, consultada el 15 de enero de 2024.

2019 Global Cybersecurity Index, en <https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf>, consultada el 15 de enero de 2024.

2021a Global Cybersecurity Index, en <https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx>, consultada el 15 de enero de 2024.

2021b Measuring digital development. Facts and figures, en: https://img.lalr.co/cms/2021/12/10163813/Facts-and-figures-2021.pdf, consultada el 15 de enero de 2024.

Intersog

2022 A Global View of Cyber Security, en <https://intersog.com/blog/global-view-of-cyber-security/>, consultada el 15 de enero de 2022.

Keohane, Robert

2012 Twenty years of institutional liberalism. International relations, 26(2), 125-138.

Kuner, Christopher

2018 International agreements, data protection, and EU fundamental rights on the international stage: Opinion 1/15, EU-Canada PNR. Common Market Law Review, 55(3).

Lewis, James

2011 Confidence-building and international agreement in cybersecurity. In Disarmament Forum (Vol. 4, pp. 51-59).

Lewis, Ted

2019 Critical infrastructure protection in homeland security: defending a networked nation. John Wiley & Sons.

Marín, Jefferson

2005 Las teorías de la guerra justa. Implicaciones y limitaciones. Revista Guillermo de Ockham, 3(2). DOI: 10.21500/22563202.478

Mendoza Enríquez, Olivio

2018 Marco jurídico de la protección de datos personales en las empresas de servicios establecidas en México: desafíos y cumplimiento. Revista IUS, 12(41), 267-291.

Moravcsik, Andrew

1992 Liberalism and international relations theory (No. 92-96). Cambridge, MA: Center for International Affairs, Harvard University.

Mordor Intelligence

2021 Cyber Warfare Market - Growth, Trends, Covid-19 Impact, and Forecasts (2022-2027), en < https://www.mordorintelligence.com/industry-reports/cyber-warfare-market>, consultada el 15 de enero de 2023.

Nye Jr., Joshep

2004 When hard power undermines soft power. New Persp. Q., 21, 13.

2011 Cyber power (pp. 1-24). Cambridge: Harvard Kennedy School, Belfer Center for Science and International Affairs.

Pfluke, Corey

2019 A history of the five eyes alliance: possibility for reform and additions: a history of the five eyes alliance: possibility for reform and additions. Comparative Strategy, 38(4), 302-315. DOI: https://doi.org/10.1080/01495933.2019.1633186

Public Safety Canada

2023 National Strategy for Critical Infrastructure, en < https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/index-en.aspx>, consultada el 15 de enero de 2024.

Schmitt, Michael

2013 Tallinn manual on the international law applicable to cyber warfare. Cambridge University Press.

Shackelford, Scott

2009 Estonia two-and-a-half years later: a progress report on combating cyber attacks. Journal of Internet Law, Forthcoming.

Sürek, Çağrı

2020 An analysis of the August War: A constructivist perspective (Master's thesis, Middle East Technical University).

Sylvester, Christine

2012 War experiences/war practices/war theory. Millennium, 40(3), 483-503. DOI: https://doi.org/10.1177/03058298124422

Sussmann, Michael

2017 The critical challenges from international high tech and computer related crime at the millennium. In Computer Crime (pp. 379-418). Routledge.

Royal Canadian Mounted Police (RCMP)

2023 "2022-23 Departmental Results Report", en <https://rcmp.ca/sites/default/files/doc/2022-2023-departmental-results-report.pdf>, consultada el 15 de enero de 2024.

Roesener, August, Bottolfson, Carl, & Fernandez, Gerry

2014 Policy for US cybersecurity. Air & Space Power Journal, 28(6), 38-54.

Swartz, Nikki

2007 Canada reviews PIPEDA. Information Management, 41(2), 8.

Tratado de Libre Comercio México, Estados Unidos y Canadá

2023 "Capitulo 19. Comercio Electrónico", Tratado de Libre Comercio México, Estados Unidos y Canadá. Gobierno de México. Gobierno de México, en < https://www.gob.mx/t-mec>, consultada el 15 de enero de 2024.

Temple-Raston, Dina

2019 How the US hacked ISIS. National Public Radio, 26.

Tonon, Graciela

2011 "La utilización del método comparativo en estudios cualitativos en ciencia política y ciencias sociales: diseño y desarrollo de una tesis doctoral". Kairos: Revista de temas sociales (27): 167-179.

U.S. Department of Justice

2018 Report Of The Attorney General's Cyber Digital Task Force, en < https://www.justice.gov/archives/ag/page/file/1076696/download>, consultada el 15 de enero de 2024.

Voo, Julia, Hemani, Irfan, Jones, Simon, DeSombre, Winnona, Cassidy, Daniel y Schwarzenbach, Anina

2020 National cyber power index 2020. Belfer Center for Science and International Affairs/Harvard Kennedy School.

Voo Julia, Hemani, Irfan y Cassidy, Daniel

2022 National cyber power index 2022. Belfer Center for Science and International Affairs/Harvard Kennedy School.

Willett, Marcus

2023 Lessons of the SolarWinds hack. In Survival April–May 2021: Facing Russia (pp. 7-25). Routledge.

Wendt, Alexander

1999 Social theory of international politics (Vol. 67). Cambridge University Press.

2004 The state as person in international theory. Review of international Studies, 30(2), 289-316.