ESCUELA NAVAL DE CADETES "ALMIRANTE PADILLA" Honor y Tradición

DERROTERO

Artículo

Soberanía Tecnológica – Ciberseguridad

Technological Sovereignty - Cybersecurity

Gonzalo Javier Rubio Piñeiro[1]*

[1] Universidad Nacional de Lanús, Remedios de Escalada, Buenos Aires, B1822, Argentina; pongui51@gmail.com
* Correspondencia: pongui51@gmail.com

Resumen: El concepto de soberanía tecnológica hace referencia, en esencia, a la capacidad de un país para controlar y gestionar sus propias tecnologías, lo cual es crucial para asegurar que sus infraestructuras críticas y datos sensibles estén protegidos frente a amenazas externas. En un mundo cada vez más interconectado, la ciberseguridad se ha convertido en un elemento clave para la soberanía nacional, ya que los ataques cibernéticos pueden poner en riesgo tanto la seguridad de los Estados como la de sus ciudadanos. Por otro lado, la soberanía tecnológica no se limita únicamente al desarrollo de tecnologías autóctonas; también implica la implementación de políticas que promuevan la independencia en la infraestructura digital, la protección de datos y la seguridad de la información. De esta manera, se busca reducir la dependencia de proveedores extranjeros y asegurar que los sistemas tecnológicos nacionales sean resilientes ante cualquier tipo de ataque o interferencia. Asimismo, es fundamental establecer normativas y estándares de ciberseguridad que garanticen la protección tanto de las empresas como de los ciudadanos, creando así un entorno digital seguro y confiable para todos los actores sociales y económicos. La soberanía tecnológica y la ciberseguridad están estrechamente interrelacionadas y son esenciales para la defensa y el bienestar de una nación en la era digital. La capacidad de un país para proteger sus activos digitales es, hoy más que nunca, un pilar fundamental para su estabilidad política, económica y social. En este contexto, los países latinoamericanos están poniendo un mayor énfasis en mejorar sus capacidades de ciberseguridad para salvaguardar sus sistemas críticos y datos sensibles de amenazas externas. La región ha experimentado una tendencia ascendente constante en el mercado cibernético, que alcanzó un valor de 5.730 millones de dólares en 2021. Sin embargo, existe una brecha importante en cuanto a habilidades digitales: solo entre el 20% y el 31% de la población posee competencias digitales fundamentales, y entre el 2% y el 12% cuenta con habilidades avanzadas en este ámbito. En particular, Brasil registró la mayor proporción de ciberataques en 2020, representando el 55,97% del total de incidentes reportados en la región. A pesar de estos desafíos, los países latinoamericanos están demostrando un fuerte compromiso para mejorar la conciencia social y cultural en la esfera cibernética. Además, están fomentando la colaboración regional, lo que facilita el intercambio de información y las mejores prácticas para fortalecer colectivamente las capacidades de ciberseguridad en la región.

Palabras clave: Soberanía Tecnológica; Ciberseguridad; Estrategias de Ciberseguridad; Capacidades Cibernéticas y Latinoamérica

Abstract: The concept of technological sovereignty refers, essentially, to a country's ability to control and manage its own technologies, which is crucial to ensure that its critical infrastructure and sensitive data are protected from external threats. In an increasingly interconnected world, cybersecurity has become a key element for national sovereignty, as cyberattacks can jeopardize the security of both states and their citizens. On the other hand, technological sovereignty is not limited to the development of domestic technologies; it also involves implementing policies that promote

check for updates

Citación: Rubio, G. Soberanía Tecnológica – Ciberseguridad. *DERROTERO* **2024**, *18*, 1–13. 10.70554/Derrotero2024.v18n02.03

Recibido: 18/04/2024
Aceptado: 06/09/2024
Publicado: 09/12/2024

Derechos de autor: © 2024 por autores. Licenciado por Escuela Naval de Cadetes "Almirante Padilla", COL. Este artículo es de libre acceso distribuido en las términos y condiciones de *Creative Commons Attribution* (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

independence in digital infrastructure, data protection, and information security. In this way, the aim is to reduce dependence on foreign suppliers and ensure that national technological systems are resilient to any form of attack or interference. Moreover, it is essential to establish cybersecurity regulations and standards that ensure the protection of both businesses and citizens, thus creating a secure and reliable digital environment for all social and economic actors. Technological sovereignty and cybersecurity are closely interconnected and are vital for the defense and well-being of a nation in the digital age. A country's ability to protect its digital assets is, now more than ever, a fundamental pillar for its political, economic, and social stability. In this context, Latin American countries are placing greater emphasis on improving their cybersecurity capabilities to safeguard their critical systems and sensitive data from external threats. The region has experienced a steady upward trend in the cybersecurity market, which reached a value of $5.73 billion in 2021. However, there is a significant gap in digital skills: only between 20% and 31% of the population has basic digital competencies, and between 2% and 12% have advanced skills in this area. In particular, Brazil recorded the highest proportion of cyberattacks in 2020, accounting for 55.97% of all reported incidents in the region. Despite these challenges, Latin American countries are demonstrating a strong commitment to improving social and cultural awareness within the cyber sphere. Additionally, they are fostering regional collaboration, which facilitates the exchange of information and best practices to collectively strengthen cybersecurity capabilities across the region.

Keywords: Technological Sovereignty; Cybersecurity; Cybersecurity Strategies; Cyber Capabilities and Latin America

1. Introducción

No se puede subestimar la importancia de la ciberseguridad, ya que es fundamental para mantener la seguridad y estabilidad de las organizaciones, redes e infraestructuras. En el mundo interconectado de hoy, donde las amenazas cibernéticas son cada vez más sofisticadas y peligrosas, las consecuencias de un ciberataque pueden ser graves y provocar importantes pérdidas financieras, daños a la reputación e incluso daños físicos. Las estrategias efectivas de ciberseguridad ayudan a las organizaciones a identificar, evaluar y gestionar amenazas potenciales, permitiéndoles mitigar los riesgos y mejorar su resiliencia.

La estrecha conexión entre ciberseguridad y soberanía tecnológica es innegable. La soberanía tecnológica, en esencia, se refiere a la capacidad de una nación para determinar de forma autónoma la utilización y el avance de la tecnología dentro de su propia jurisdicción, libre de cualquier influencia o control externo. La ciberseguridad desempeña un papel fundamental en la salvaguardia de la soberanía tecnológica, ya que permite a los países proteger sus sistemas críticos y datos confidenciales de amenazas externas, garantizando así su capacidad para tomar decisiones independientes con respecto a la tecnología dentro de sus fronteras. En una era en la que los ciberataques aumentan tanto en frecuencia como en complejidad, la ciberseguridad se ha convertido en un requisito previo indispensable para la soberanía, lo que obliga a las naciones a adoptar medidas proactivas para preservar su soberanía tecnológica.

Como resultado de las repercusiones que la pandemia de Covid-19 ha tenido en el ámbito digital, los países se han visto obligados a implementar una serie de medidas, políticas e iniciativas con el fin de proteger sus activos más vulnerables frente a las diversas amenazas y riesgos que surgen en el ciberespacio. Dado que este tema es de gran relevancia y actualidad, resulta fundamental realizar una evaluación detallada de las metodologías de ciberseguridad adoptadas por países como Argentina, Brasil, Chile, Colombia, México y Perú. El objetivo principal de este estudio es profundizar en la comprensión de las estrategias implementadas, que, a primera vista, parecen no solo reforzar la protección de la infraestructura crítica, sino también fomentar esfuerzos de colaboración global en el ámbito de la ciberseguridad.

En este artículo se adoptó una metodología mixta, integrando análisis cuantitativos y cualitativos. El análisis cuantitativo se estructuró en dos fases. En la primera, se emplearon indicadores clave para proporcionar una visión general de los países seleccionados, abarcando datos a nivel individual y nacional, los cuales se detallan en la sección de descripción general del estudio. En la segunda fase, se realizó un análisis cuantitativo más exhaustivo utilizando el Índice Nacional de Seguridad Cibernética (NCSI). Este índice global mide la preparación de los países para enfrentar amenazas cibernéticas y gestionar incidentes en el ciberespacio de manera eficiente. Además, el NCSI actúa como una base de datos pública de materiales de evidencia y fomenta el desarrollo de capacidades nacionales en ciberseguridad.

Para el análisis cualitativo, se examinaron las estrategias nacionales de ciberseguridad. Estas estrategias fueron extraídas del Repositorio Nacional de Estrategias de Ciberseguridad, una recopilación realizada por la Unión Internacional de Telecomunicaciones.

2. Soberanía Tecnológica - Ciberseguridad

Según el informe de Naciones Unidas de 2021: "La ciberseguridad en las organizaciones del sistema de Naciones Unidas" no existe una definición de ciberseguridad universalmente aceptada ni un consenso mundial sobre lo que abarca exactamente el término. Por esta razón, en el mencionado informe, los Inspectores decidieron utilizar la definición de ciberseguridad elaborada por la Unión Internacional de Telecomunicaciones (UIT), que fue aceptada por las organizaciones participantes y que se detalla a continuación:

El conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, enfoques de la gestión del riesgo, medidas, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno. Los activos de la organización y los usuarios son los dispositivos informáticos conectados, los usuarios, los servicios/aplicaciones, los sistemas de comunicaciones, las comunicaciones multimedios, y la totalidad de la información transmitida y/o almacenada en el ciberentorno. La ciberseguridad garantiza que se alcancen y mantengan las propiedades de seguridad de los activos de la organización y los usuarios contra los riesgos de seguridad correspondientes en el ciberentorno. Las propiedades de seguridad incluyen una o más de las siguientes: disponibilidad; integridad, que puede incluir la autenticidad y el no repudio; y confidencialidad. (Flores Callejas and Lozinskiy 2021)

El informe Latin America Threat Outlook, publicado recientemente por Kaspersky, analiza datos correspondientes a dos períodos: de junio de 2022 a julio de 2023 y de junio de 2021 a julio de 2022. Este documento revela que, aunque el comportamiento delictivo en la región se ha mantenido relativamente estable, se ha registrado un notable aumento en los ataques de malware dirigidos tanto a computadoras como a dispositivos móviles. Destacan especialmente los intentos de ataques de phishing, que experimentaron un alarmante incremento del 617%, y los troyanos bancarios, que aumentaron un 50%. Los sectores más afectados por estas amenazas incluyen el gobierno, las industrias financieras y los usuarios de Internet en general.

Los expertos atribuyen este incremento de actividades fraudulentas a la reactivación económica posterior a la pandemia. Además, el uso de herramientas basadas en inteligencia artificial ha facilitado la creación automatizada de contenido fraudulento, intensificando aún más estas amenazas.

La gravedad de este fenómeno se evidencia aún más considerando la creciente frecuencia de los ataques cibernéticos en una región como América Latina, que todavía se encuentra en etapas iniciales de desarrollo y aplicación de políticas de ciberseguridad. Aunque países como Argentina, Brasil, Chile, Colombia, México y Perú han comenzado a implementar políticas de ciberseguridad relativamente recientes, estas iniciativas representan un gran potencial para impulsar avances significativos en el fortalecimiento de la seguridad cibernética en la región.

3. La importancia de las estrategias de ciberseguridad en el avance de las capacidades cibernéticas

Para mejorar la capacidad de un país para resistir las amenazas digitales, es crucial implementar iniciativas educativas sociales y culturales que se centren en mejorar las habilidades de ciberseguridad y promover la conciencia cibernética. Este enfoque puede ser a la vez muy eficaz y rentable para las naciones en cuestión. Sin embargo, es importante señalar que este enfoque por sí solo no aborda plenamente la necesidad de desarrollar capacidades cibernéticas nacionales, lo que exige una perspectiva estratégica unificada e integral.

Surge entonces el concepto de "gobernanza de la ciberseguridad", que abarca una perspectiva integral e interconectada sobre la protección de redes, sistemas, servicios e infraestructuras dentro de la sociedad. El concepto de gobernanza abarca una amplia gama de elementos, como instituciones, esfuerzos políticos, iniciativas, programas y varios otros mecanismos, tanto formales como informales. Estos componentes forman colectivamente una red interconectada de capacidades y responsabilidades de ciberseguridad. Para consolidar sus capacidades cibernéticas, un país debe contar con una estrategia nacional de ciberseguridad.

La región no solamente participa en iniciativas de ciberseguridad a nivel nacional, sino que también participa activamente en esfuerzos internacionales, demostrando un alto nivel de madurez en aspectos culturales y sociales. Como por ejemplo la participación en la plataforma CSIRT (Equipo de respuesta a incidentes de seguridad informática) que sirve como un espacio de colaboración para que los países se involucren y participen activamente.

En un esfuerzo de colaboración, los estados mencionados participan activamente en iniciativas de ciberseguridad bajo el paraguas de la Organización de Estados Americanos (OEA) (OEA 2023). Asimismo, la OEA ha desempeñado un papel fundamental al ayudar a Colombia (2011 y 2016), Chile (2017), México (2017) y Brasil (2018 y 2020) en el desarrollo e implementación de sus estrategias inaugurales de ciberseguridad.

Por otro lado, el reconocimiento del ciberespacio como quinto dominio para operaciones militares por parte de la OTAN en 2016 es una declaración significativa de los peligros potenciales asociados con la militarización de este ámbito.

Asimismo, la noción de soberanía tecnológica abarca la capacidad de una nación o comunidad para gobernar y dirigir de forma independiente sus propios avances tecnológicos, libre de dependencias o influencias externas. Está estrechamente vinculado al concepto de soberanía nacional, que denota la prerrogativa de una nación de ejercer control y autoridad dentro de sus fronteras territoriales. En nuestro panorama global interconectado, la preservación de la soberanía tecnológica adquiere una importancia primordial para defender la autonomía de una nación y salvaguardar su seguridad. Delinea el grado en que un país puede ejercer control sobre su infraestructura digital y proteger información confidencial. En consecuencia, la ciberseguridad asume un papel fundamental en la salvaguardia y el aumento de la soberanía tecnológica.

4. Un examen de la preparación digital de la región latinoamericana

Para lograr una comprensión más profunda de las estrategias nacionales de ciberseguridad y los factores legales, políticos, económicos y sociales subyacentes que las impulsan, es crucial examinar las condiciones generales de estos países utilizando varios indicadores. Comencemos comparándolos en función del Índice de Desarrollo Humano (IDH) (Human Development Reports 2023), que evalúa la esperanza de vida, la educación y el Producto Nacional Bruto (PNB). Chile toma el liderazgo en el ranking del IDH y se ubica en el puesto 43 a nivel mundial con una puntuación de 0,851 puntos. Le siguen de cerca Argentina (46), México (74), Perú (79), Colombia (83) y Brasil (84) (Tabla 1).

Tabla 1. Comparación del Índice de Desarrollo Humano (IDH)

Clasificación IDH	País	Índice de Desarrollo Humano (IDH)	Esperanza de vida (años)	Años de escolaridad esperados (años)	Años medios de escolaridad (años)	Ingreso Nacional Bruto (INB) per cápita ($ PPA de 2020)	Clasificación de INB per cápita menos clasificación del IDH
43	Chile	0.851	80.2	16.4	10.6	23,261	16
46	Argentina	0.845	76.7	17.7	10.9	21,190	16
74	México	0.779	75.1	14.8	9.0	19,130	-8
79	Perú	0.777	76.7	15.0	8.9	12,252	-19
83	Colombia	0.767	77.3	14.4	8.5	14,257	1
84	Brasil	0.765	75.9	15.4	8.4	14,263	1

Fuente: Contribución propia del autor basada en datos de Human Development Index (HDI) 2020.

Debido a que el IDH proporciona una visión general del desarrollo humano, es esencial considerar indicadores adicionales que están estrechamente vinculados a los dispositivos digitales para una comprensión más integral.

El Instituto para el Desarrollo Gerencial (IMD) (International Institute for Management Development (IMD) 2023) de Lausana, Suiza, elabora el Índice Mundial de Competitividad Digital, el cual evalúa la preparación de un país en tres áreas clave: conocimiento, tecnología y preparación para el futuro. El informe publicado en 2021 destaca que los países con mejores clasificaciones en el pilar de preparación para el futuro tienden a obtener resultados más positivos en general, lo que subraya la importancia de la adaptabilidad frente a un panorama en constante cambio. En este sentido, Chile lidera la región y ocupa el puesto 39, seguido por Brasil (51), México (56), Perú (57), Colombia (59) y Argentina (61). Al analizar los pilares individuales, se observa que la mayoría de los países destacan en el ámbito de la tecnología, mientras que Chile y Perú se distinguen especialmente en el área del conocimiento (Tabla 2).

Tabla 2. Comparación del Índice de Competitividad Digital Mundial (ICDM)

Clasificación ICDM	País	Índice de Competitividad Digital Mundial (ICDM) - Valor	Conocimiento - Valor	Tecnología - Valor	Preparación para el futuro - Valor
39	Chile	61.796	49	35	36
51	Brasil	51.478	51	55	45
56	México	48.736	54	57	51
57	Perú	47.227	59	60	53
59	Colombia	45.454	56	60	53
61	Argentina	43.639	55	62	52

Fuente: Contribución propia del autor basada en datos de World Digital Competitiveness Ranking 2021.

La Clasificación de la Unión Internacional de Telecomunicaciones (UIT) (Unión Internacional de Telecomunicaciones (UIT) 2023) constituye otro recurso valioso para analizar la penetración de Internet en la sociedad, ya que ofrece una visión detallada sobre su amplio uso y la medida en que ha permeado diversos sectores. Al examinar el porcentaje de personas que interactúan con Internet en relación con la población general, se obtiene información significativa. En este sentido, Chile lidera el ranking con un 90%, seguido de cerca por Argentina con un 88%. A continuación, Brasil, México, Perú y Colombia presentan cifras de 81%, 76%, 75% y 73%, respectivamente. Una diferencia importante respecto al año anterior es que, en esa ocasión, Argentina ocupaba una posición más destacada que Chile. Además, al desglosar los datos por grupos de edad, se aprecian variaciones interesantes en la proporción de usuarios de Internet. Por ejemplo, en Argentina y Brasil, el 95% y el 94%

de las personas entre 15 y 24 años participan activamente en actividades en línea, seguidos de cerca por México (93%), Perú (91%) y Colombia (88%). Es particularmente revelador observar la presencia de usuarios de Internet dentro del grupo de edad de mayores de 75 años, especialmente en Argentina, donde alcanza un 42%, seguido de Brasil con un 23% y México con un 14%. Este dato subraya la creciente inclusión digital de personas de edad avanzada en la región (Tabla 3).

Tabla 3. Comparación del Índice de Competitividad Digital Mundial (ICDM)

País	Uso individual de internet (Porcentaje)	Rango de edad				Uso individual de internet (Porcentaje)
		25-74	15-24	Menores de 15	Mayores de 75	
Chile (2021)	90%	N/D	N/D	95%	N/D	82% (2020)
Argentina (2022)	88%	90%	95%	85%	42%	85% (2021)
Brasil (2022)	81%	80%	94%	89%	23%	74% (2021)
México (2021)	76%	73%	93%	79%	14%	72% (2020)
Perú (2022)	75%	73%	90%	78%	19%	65% (2021)
Colombia (2022)	73%	72%	88%	74%	19%	65% (2021)

Fuente: Contribución propia del autor basada en datos de International Telecommunication Union (ITU).

Urbanovics and Guajardo (2022) afirman en Estrategias de ciberseguridad en los países latinoamericanos – un análisis comparativo que, en términos de competencias digitales, apenas entre el 20% y el 31% de la población posee habilidades fundamentales, mientras que una fracción aún más pequeña, que oscila entre el 2% y el 12%, cuenta con competencias avanzadas. Estas cifras subrayan el hecho de que, a pesar de los avances en la infraestructura tecnológica dentro de los países examinados, las personas no pueden seguir el ritmo de estas mejoras. En consecuencia, esta situación ejerce una inmensa presión sobre la sociedad, dejando a quienes carecen de las habilidades digitales adecuadas susceptibles a ataques cibernéticos y vulnerables en su existencia en línea.

El mercado cibernético en esta región en particular está experimentando una trayectoria ascendente constante en términos de su valor. En 2021, el mercado de la ciberseguridad en América Latina estaba valorado en USD 5.730 millones. Se estimó que de 2022 a 2027, el mercado general crecería a una tasa anual compuesta de alrededor del 11,8%, superando los USD 10.000 millones para 2027 (Statista 2023b).

En 2020, Brasil experimentó la mayor proporción de ciberataques entre los países de América Latina, representando el 55,97% del total. Le siguieron México y Colombia con 27,86% y 7,33% respectivamente. Sorprendentemente, a pesar de ser el país más afectado, Brasil no priorizó su gasto en tecnología de la información (TI), como se muestra en la Figura 1. Al observar la variación en el gasto en TI en 2021, Argentina alcanzó el mayor aumento con un 10,4%, seguido de México (10%) y Perú (9%) (Statista 2023a). Esto genera preocupación para Brasil, especialmente considerando que el sector público administra la mayor parte de la infraestructura crítica del país, lo que la hace aún más vulnerable a los ataques cibernéticos.

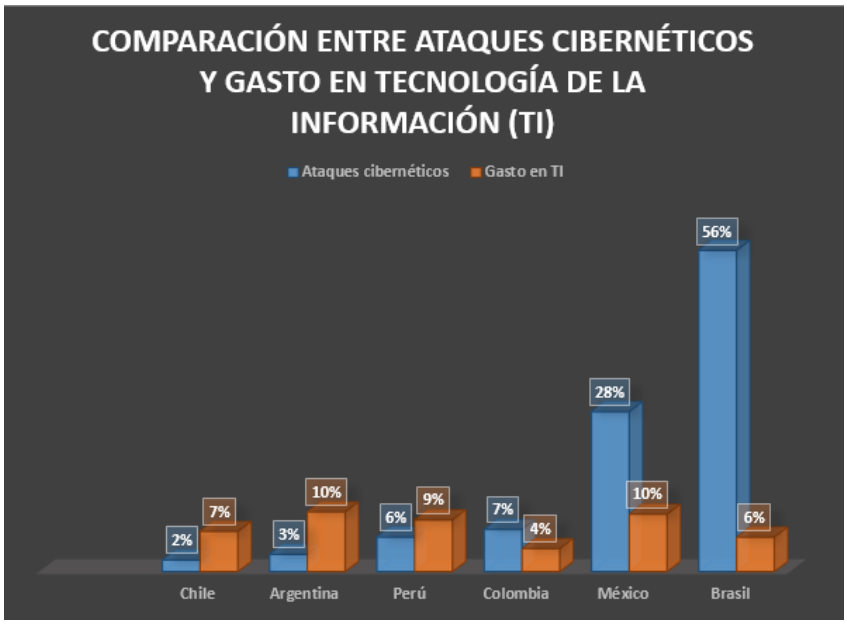

Figura 1. Comparación entre Ataques cibernéticos y Gasto en tecnología de la información (TI)
Fuente: Contribución propia de los autores basada en datos de Statista

5. Comparación de las estrategias de ciberseguridad

La Fundación Academia de Gobernanza Electrónica de Estonia ha desarrollado un índice que tiene como objetivo evaluar la preparación de los países para mitigar los ataques y amenazas cibernéticos. Este índice sirve como plataforma para el intercambio de información entre países, ya que incluye antecedentes que complementan los datos proporcionados por cada país. El Índice Nacional de Ciberseguridad (NCSI) se centra principalmente en las medidas de ciberseguridad implementadas por el gobierno central. Sigue una estructura jerárquica, que consta de tres categorías, doce capacidades y un total de cuarenta y seis variables, que son reportadas por las contrapartes de cada país. El indicador resultante es un valor numérico que va de 0 a 100 (Figura 2).

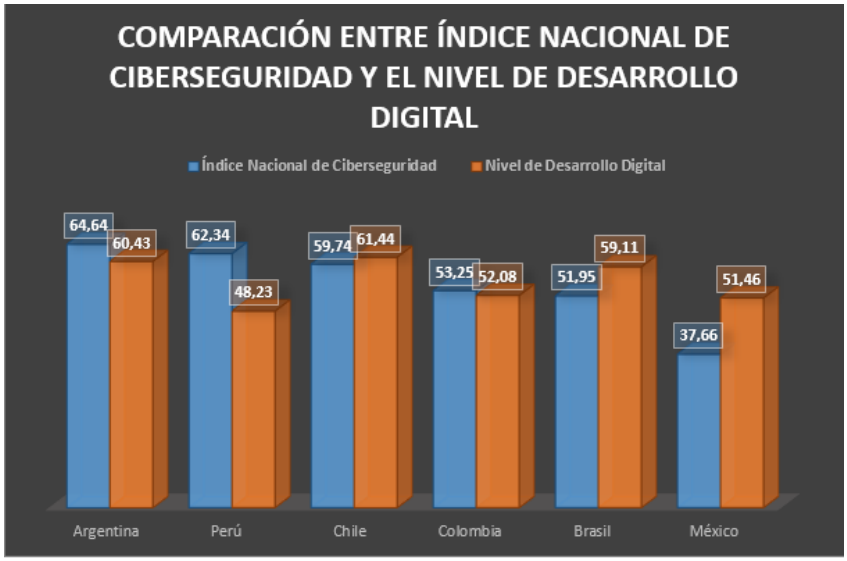

Figura 2. Comparación entre Ataques cibernéticos y Gasto en tecnología de la información (TI)
Fuente: Contribución propia de los autores basada en datos del National Cyber Security Index (NCSI)

Argentina emerge como la fuerza dominante en el Índice Nacional de Ciberseguridad (NCSI), con un puntaje de 64,64 puntos. Detrás, Perú ocupa el segundo lugar con 62,34 puntos, mientras que Chile lo sigue de cerca con 59,74 puntos. Chile adquiere una posición de privilegio con 61,44 en el Nivel de Desarrollo Digital, seguido por Argentina con 60,43 y Brasil con 59,11. Cabe destacar que, pese a que Perú recientemente ha formulado su propia estrategia nacional de ciberseguridad y ostenta el último lugar en el Nivel de Desarrollo Digital con 48,23 puntos, se encuentra mejor posicionado en el NCSI que Chile, Colombia, Brasil y México por la profundidad de sus medidas políticas respecto a la temática.

Al realizar un análisis más exhaustivo de los distintos componentes del índice, es posible determinar el nivel de madurez exhibido por cada país individualmente. Tomando de base los indicadores generales de ciberseguridad nos adentraremos comparar a los países analizados a través de los indicadores de gestión de incidentes y crisis (Figura 3, 4).

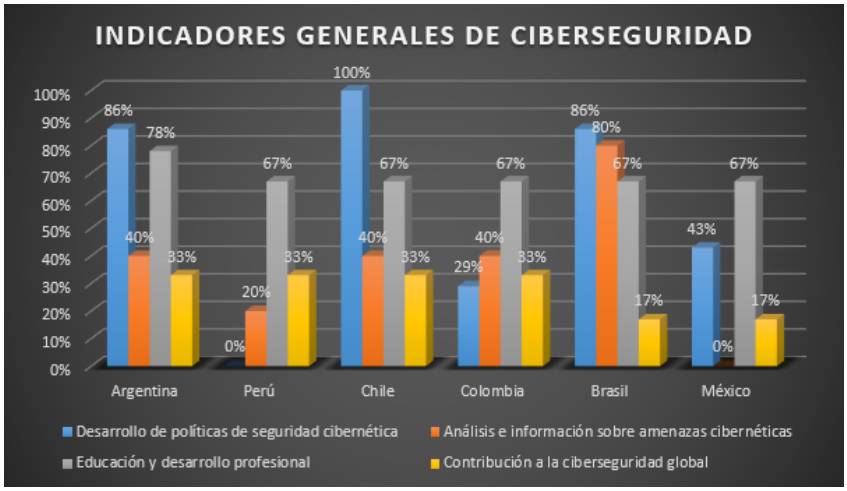

Figura 3. Indicadores generales de ciberseguridad e indicadores de gestión de incidentes y crisis
Fuente: Contribución propia de los autores basada en datos del National Cyber Security Index (NCSI)

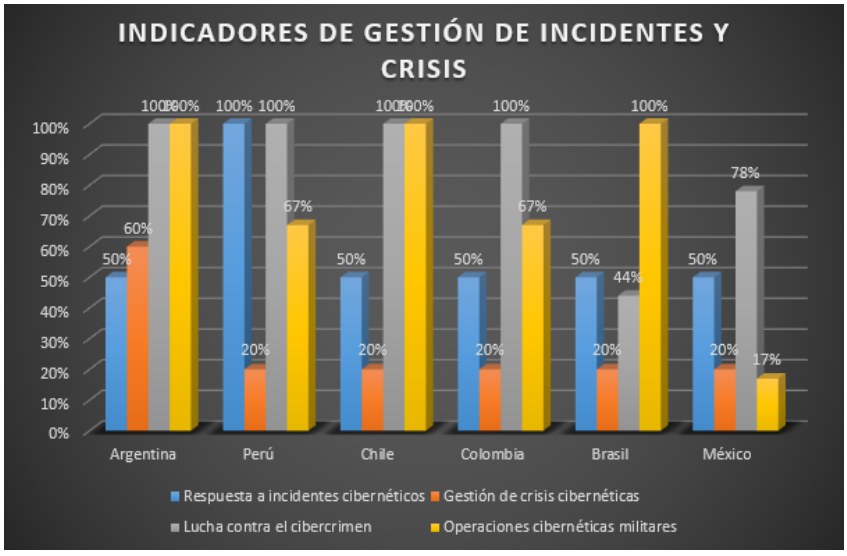

Figura 4. Indicadores generales de ciberseguridad e indicadores de gestión de incidentes y crisis
Fuente: Contribución propia de los autores basada en datos del National Cyber Security Index (NCSI)

El conjunto inicial de indicadores se enfoca principalmente en aspectos generales de la política de ciberseguridad, así como en la respuesta ante incidentes cibernéticos. Dentro de esta categoría, uno de los puntos más relevantes es la capacidad de los países para responder de manera eficaz a los incidentes cibernéticos y gestionar crisis en este ámbito,

un área en la que ninguno de los países analizados ha alcanzado una preparación completa. Sin embargo, es importante resaltar que todos los países estudiados han creado una unidad específica para la respuesta a incidentes cibernéticos. Por ejemplo, el Centro de Respuesta a Incidentes Cibernéticos (CERT) de México fue establecido el 1 de junio de 2010, mientras que Chile formó unidades gubernamentales especializadas en ciberseguridad, incluido el Departamento CSIRT, a través de la Resolución Exenta N.º 5.006 en agosto de 2019. Brasil también mantiene unidades CSIRT y CERT, mientras que Colombia y Perú cuentan con sus propias unidades CERT.

En lo que respecta a la lucha contra el cibercrimen, Chile ha adoptado un enfoque integral, estableciendo no solo una unidad especializada en ciberdelincuencia, sino también una unidad de análisis forense digital. Además, ha implementado un servicio de contacto disponible las 24 horas, los 7 días de la semana, para gestionar asuntos internacionales relacionados con el cibercrimen. Cabe destacar que, al igual que Chile, todos los países en cuestión han desarrollado marcos legales que penalizan los delitos cibernéticos dentro de sus respectivas legislaciones nacionales (Interpol 2021).

En este contexto, Argentina fue pionero en la promulgación de una ley específica para el tratamiento de los delitos cibernéticos. A través de la Ley N.º 26.388, aprobada el 24 de junio de 2008, Argentina modificó su Código Penal y estableció sanciones para diversos delitos cibernéticos, tales como la interceptación de comunicaciones, el acceso no autorizado a sistemas informáticos, el daño a sistemas informáticos, el fraude, la falsificación electrónica, la interrupción de las comunicaciones y la manipulación de pruebas digitales.

Por otro lado, Brasil se distingue por mantener una unidad dedicada al análisis de amenazas cibernéticas y por operar un sitio web de ciberseguridad, el cual está bajo la supervisión de una autoridad pública. Esta medida refuerza el compromiso del país con la protección de su infraestructura digital y la lucha contra el cibercrimen, complementando los esfuerzos de los otros países de la región. En cuanto a las operaciones cibernéticas militares, Brasil y Chile se han destacado por establecer unidades especializadas para este fin, demostrando su capacidad a través de varios ejercicios en el ámbito de las operaciones cibernéticas militares. Es importante subrayar que todos los países examinados han participado activamente en ejercicios internacionales relacionados con este tipo de operaciones. Argentina y Chile participaron en la Operación Panamax 2016, mientras que los demás países se unieron en las ediciones de la Operación Panamax 2018 y 2022.

En términos de formulación de políticas, Chile se destaca como el país más avanzado, seguido por Argentina. Chile fue el primero en establecer una unidad dedicada a la política de ciberseguridad a través del Decreto Supremo N.º 533/2015, que creó el Comité Interministerial de Ciberseguridad (CICS) (Ciberseguridad 2024). Esta iniciativa fue reforzada por el Decreto Supremo N.º 579/2019, que creó una nueva comisión técnica con facultades consultivas en materia de ciberseguridad. De manera similar, Argentina y Brasil también han establecido unidades operativas en este ámbito: la Dirección Nacional de Ciberseguridad de Argentina, creada por el Jefe de Gabinete mediante la DA 103/2019, y el Departamento de Seguridad de la Información de Brasil, establecido por el Decreto 9668 de 2019 (Tabla 5).

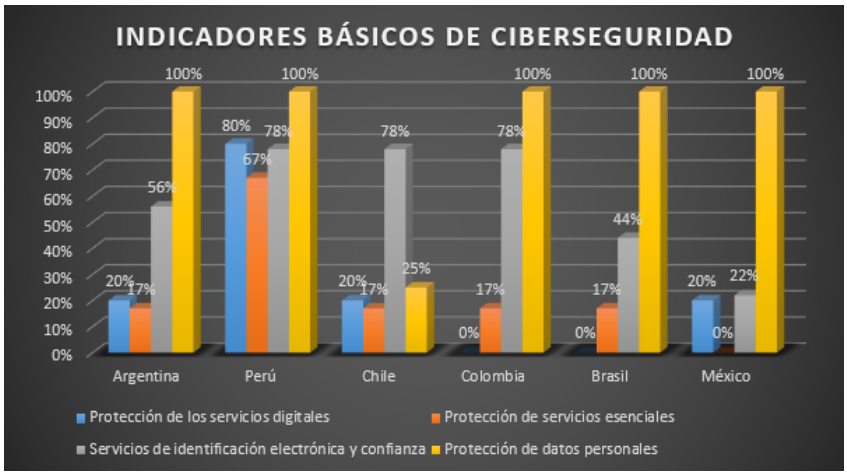

Figura 5. Indicadores generales de ciberseguridad e indicadores de gestión de incidentes y crisis
Fuente: Contribución propia de los autores basada en datos del National Cyber Security Index (NCSI)

El segundo conjunto de indicadores, que se refieren principalmente a cuestiones de servicio y protección de datos. Una tendencia notable en todos los países es una disminución en el nivel de preparación en estos aspectos de la política de ciberseguridad. Sin embargo, cabe señalar que la protección de datos personales ha alcanzado un estado de plena preparación en Argentina, Colombia, México y Perú. Por otro lado, todavía hay algunos países que no han implementado ninguna política para la protección de los servicios digitales y los servicios esenciales. Brasil y Colombia carecen de políticas para el primero, mientras que México carece de políticas para el segundo. En términos de fijación de estándares de ciberseguridad para el sector público, Perú están a la vanguardia en la protección de servicios digitales.

Las autoridades públicas de Argentina han implementado un Modelo de Política de Seguridad de la Información, mientras que en Chile se han implementado medidas específicas a través del Decreto Presidencial N° 8 de 2018 sobre Ciberseguridad. De manera similar, México emitió la Guía de Ciberseguridad para Instalaciones Públicas en 2018. Cuando se trata de educación en ciberseguridad, en la mayoría de los países se encuentran disponibles títulos de licenciatura y maestría en ciberseguridad, pero no existen programas de nivel de doctorado. Sin embargo, esto no significa que no existan oportunidades para realizar una investigación de nivel doctoral en ciberseguridad en esos países. Aunque no haya programas de doctorado especializados, aún se pueden realizar estudios de doctorado en disciplinas relacionadas, como informática, ingeniería informática o seguridad de la información.

Argentina, Brasil, Chile, Colombia, México y Perú, se encuentran en las primeras etapas de cooperación internacional en términos de esfuerzos globales de ciberseguridad. A medida que emergen como nuevas potencias cibernéticas, están comenzando a establecer políticas y marcos regulatorios para abordar los desafíos de seguridad cibernética. Sin embargo, es cierto que, en comparación con otras regiones del mundo, la contribución de estos países en términos de esfuerzos globales de ciberseguridad aún se considera baja. Esto puede deberse a varios factores, como la falta de recursos financieros y técnicos, la necesidad de mayor conciencia y capacitación en ciberseguridad, y la falta de una infraestructura sólida en este campo.

No obstante, la tendencia general muestra un aumento en los esfuerzos de cooperación internacional y una mayor conciencia sobre la importancia de la seguridad cibernética. Estos países están participando en iniciativas regionales, como la creación de centros de respuesta a incidentes cibernéticos y la celebración de conferencias y encuentros para intercambiar conocimientos y mejores prácticas.

La naturaleza compleja de las estrategias nacionales, que se basan en los factores analizados permiten inferir que Argentina, Perú y Chile emergen como líderes entre los

países examinados en las clasificaciones globales. Asimismo, al analizar las estrategias implementadas, se pueden discernir los perfiles de cada país. A saber:

6. Argentina

Argentina ha dado un paso significativo al establecer un plan nacional integral de ciberseguridad que promueve la concientización y la educación en este ámbito. La formación de profesionales, técnicos e investigadores y la colaboración con la ciberindustria son elementos clave de esta iniciativa. Estas medidas contribuyen a fortalecer la seguridad en el entorno digital y proteger los sistemas y datos tanto a nivel individual como a nivel nacional.

7. Brasil

La estrategia nacional de ciberseguridad de Brasil se enfoca en el sector público, buscando establecer requisitos mínimos de ciberseguridad para las entidades públicas y promoviendo la defensa y el intercambio de información para combatir los delitos cibernéticos. Estas medidas son importantes para fortalecer la seguridad cibernética en el ámbito público y proteger los sistemas y datos de las amenazas digitales.

8. Chile

Chile muestra un compromiso decidido con la colaboración internacional en ciberseguridad y considera la política cibernética como una parte integral de su política exterior. Su enfoque incluye abogar por regulaciones globales, participar en foros de gobernanza y promover la cooperación bilateral y multilateral. Estas acciones son fundamentales para promover la confianza y garantizar la seguridad en el ciberespacio a nivel mundial.

9. Colombia

En Colombia se ha implementado una estrategia de defensa holística que abarca diversos aspectos como medidas de ciberseguridad, gestión de incidentes y análisis forense digital. Esta estrategia reconoce la importancia de la infraestructura cibernética como un componente vital de la infraestructura crítica y apunta a salvaguardarla mediante la prevención proactiva, la respuesta rápida y el enjuiciamiento efectivo de los delitos cibernéticos. Estas medidas proactivas desempeñan un papel crucial en el fortalecimiento del panorama de ciberseguridad de la nación, garantizando la protección de sistemas y datos valiosos contra las amenazas digitales siempre presentes.

10. México

En México, se considera la prevención del delito cibernético como una prioridad y se aborda de manera integral. Esto incluye fomentar una cultura de ciberseguridad, mejorar las capacidades cibernéticas y fortalecer el marco legal y la autorregulación. Estas acciones son fundamentales para proteger a los ciudadanos y a las organizaciones de los riesgos y amenazas en el entorno digital.

11. Perú

La Estrategia Nacional de Ciberseguridad de Perú incluye medidas como la creación de centros de respuesta a incidentes cibernéticos, programas de concientización y capacitación, y la promoción de estándares de seguridad en infraestructuras críticas. Estas acciones buscan fortalecer la seguridad en el ciberespacio a través de la colaboración entre el sector público y privado y proteger los sistemas y datos de posibles amenazas cibernéticas.

12. Conclusiones

A la luz del aumento de las amenazas cibernéticas y la creciente importancia del ámbito digital para fortalecer las capacidades nacionales e internacionales, la formulación de estrategias nacionales integrales y la creación de unidades especializadas en ciberseguridad son más urgentes que nunca. Aunque las naciones emergentes aún se encuentran en

proceso de ponerse al día con sus contrapartes más avanzadas, las tendencias recientes muestran un claro compromiso con el desarrollo de políticas cibernéticas. En particular, los países latinoamericanos han demostrado un interés sin precedentes en aumentar la conciencia social y cultural sobre la ciberseguridad, al tiempo que fomentan la colaboración regional para fortalecer sus capacidades y facilitar el intercambio de información y mejores prácticas.

Un análisis detallado evidencia que estas naciones son especialmente vulnerables a los ciberataques debido a factores como el aumento de usuarios de Internet y redes sociales, junto con una infraestructura institucional y regulatoria aún insuficiente. Brasil, a pesar de ser el país más afectado por los ciberataques en la región, presenta un gasto relativamente bajo en tecnología de la información (TI) en comparación con otros países de América Latina.

De acuerdo con el Índice Nacional de Seguridad Cibernética (NCSI) y el Índice de Nivel de Desarrollo Digital, países como Argentina, Perú y Chile destacan por su desempeño general. Sin embargo, todavía enfrentan desafíos en áreas clave como la protección de servicios esenciales, la salvaguarda de datos personales y la gestión de crisis cibernéticas. Brasil, aunque sufre el mayor número de ataques, lidera en el análisis de amenazas y operaciones cibernéticas militares. Por su parte, Chile y Argentina, que encabezan el ranking del NCSI, adoptan enfoques más integrales que incluyen educación en seguridad digital, detección de delitos cibernéticos, creación de marcos regulatorios y promoción de la colaboración internacional e industrial.

En términos de desarrollo de estrategias nacionales de ciberseguridad, los países analizados presentan niveles variados de preparación. Algunos carecen de un plan definido, pero el potencial para avanzar en este ámbito es significativo. La determinación de los gobiernos para afrontar este desafío se ha intensificado, especialmente tras la pandemia de COVID-19, que subrayó la necesidad de enfoques colaborativos y coordinados.

Por otra parte, el concepto de soberanía tecnológica, entendido como la capacidad de una nación para gestionar y controlar de manera autónoma su desarrollo tecnológico, está estrechamente vinculado a la soberanía nacional. En un mundo interconectado, la soberanía tecnológica es esencial para garantizar la autonomía y seguridad de una nación, pues define el grado de control sobre su infraestructura digital y la protección de información sensible. En este contexto, la ciberseguridad desempeña un papel fundamental para preservar y fortalecer esta soberanía.

Para promover la independencia tecnológica mediante estrategias sólidas de ciberseguridad, se pueden adoptar medidas como:

- Elaboración de estrategias nacionales integrales de ciberseguridad: Definir objetivos claros y prioridades para proteger sistemas críticos e información confidencial.
- Reducción de la dependencia de tecnologías extranjeras: Invertir en el desarrollo de tecnologías nacionales y en el fortalecimiento de la infraestructura digital local.
- Fomento de una cultura de ciberdefensa: Priorizar la educación y concienciación en ciberseguridad y promover la colaboración entre gobiernos, industrias y academia.
- Creación de marcos legales y regulatorios sólidos: Combatir las amenazas cibernéticas respetando al mismo tiempo los derechos de privacidad.
- Impulso de la colaboración internacional: Intercambiar información y abordar colectivamente los desafíos de la ciberseguridad global mientras se refuerza la independencia tecnológica.

La implementación de estas medidas permitirá a las naciones proteger su independencia tecnológica, controlar su infraestructura digital y salvaguardar su autonomía y seguridad en la era digital.

Contribuciones de los autores:
Gonzalo Javier Rubio Piñeiro: Conceptualización, Metodología, Validación, Análisis formal, Investigación, Redacción - borrador original, Redacción - revisión y edición.

Financiación: Esta investigación no recibió financiación externa.

Conflicto de Intereses: Los autores declaran no tener conflictos de interés.

Referencias

Ciberseguridad, A. (2024). Comité interministerial de ciberseguridad (cics).
Flores Callejas, J., A. A. and Lozinskiy, N. (2021). *La ciberseguridad en las organizaciones del sistema de las Naciones Unidas (JIU/REP/2021/3)*. Naciones Unidas, Ginebra.
Human Development Reports (2023). United Nations Development Program - Human Development Report Office.
International Institute for Management Development (IMD) (2023). World Digital Competitiveness Ranking (WDCR).
Interpol (2021). *Guía sobre la Estrategia Nacional contra la Ciberdelincuencia*. JAIF, Lyon.
OEA (2023). *Guía práctica para CSIRTS - Volumen 2*. CSIRTAmericas Network, Washington D. C.
Statista (2023a). Countries in Latin America most targeted by cyber attacks in 2020.
Statista (2023b). Value of the cybersecurity market in Latin America in 2021 and 2027.
Unión Internacional de Telecomunicaciones (UIT) (2023). ITU Statistics - Digital Development Dashboard.
Urbanovics, A. and Guajardo, R. (2022). Estrategias de ciberseguridad en los países latinoamericanos – un análisis comparativo. *Acta Hispanica*, IV:89–104.

Biografía de los Autores

Gonzalo Javier Rubio Piñeiro Magíster en Defensa Nacional; Profesor de la Universidad Nacional de Lanús, Argentina

Descargo de responsabilidad/Nota del editor: Las declaraciones, opiniones y datos contenidos en todas las publicaciones son únicamente responsabilidad de los autores y colaboradores individuales y no reflejan necesariamente las opiniones de DERROTERO y/o de los editores. DERROTERO y/o los editores se deslindan de cualquier responsabilidad por daños o perjuicios a personas o bienes que puedan surgir como resultado de las ideas, métodos, instrucciones o productos mencionados en el contenido. Se recomienda a los lectores verificar de manera independiente la información antes de basarse en ella.