https://doi.org/10.14232/actahisp.2022.0.89-104

ESTRATEGIAS DE CIBERSEGURIDAD EN LOS PAÍSES LATINOAMERICANOS – UN ANÁLISIS COMPARATIVO

ANNA URBANOVICS – RODRIGO GUAJARDO SANTANA

Universidad Nacional de Servicio Público, Hungría

Resumen: Siguiendo a los países desarrollados, los países latinoamericanos comienzan a prestar cada vez más atención al desarrollo de sus capacidades en ciberseguridad. Cada vez más países de la región crean su propia estrategia nacional de ciberseguridad, estableciendo los principales objetivos e intereses, así como definiendo los principales desafíos y amenazas. El estudio tiene como objetivo analizar y comparar estas estrategias publicadas por los principales estados de la región. El artículo parte de un diseño de investigación basado en métodos mixtos. La metodología utilizada consiste, en su mayor parte, en el análisis de datos secundarios soportados por bases de datos internacionales, así como el análisis sistemático de las estrategias mediante técnicas de análisis documental. Los resultados esperados, por lo tanto, tienden a resumir las principales estructuras de estas estrategias –incluyendo intereses y desafíos centrales que se definen con respecto a los estados estudiados– identificando así patrones comunes de las estrategias considerando el contexto político e internacional de la región y hacer sugerencias para desarrollos futuros mediante la comparación de la situación actual y las principales estructuras de estos países.
Palabras Clave: Latinoamérica, ciberseguridad, análisis estratégico, análisis documental, cibercapacidades.

Abstract: Following the developed countries, Latin American countries start to pay more attention to developing their cyber capabilities. In alignment with these, more and more countries from the region create their own national cybersecurity strategy, stating the main targets, interests and defining the main challenges and threats. The study aims to analyze and compare these strategies issued by the leading states of the region. The article has a mixed methods research design. The methodology used mostly consists of secondary data analysis based on international databases as well as the systematic analysis of the strategies by document analysis techniques. The expected results therefore tend to summarize the main structures of these strategies –including the principal interests and defining challenges with respect to the studied states– identify common patterns of the strategies considering the political and international context of the region and make suggestions for future developments by comparing the current situation and main structures of these countries.
Keywords: Latin America, Cybersecurity, Strategy Analysis, Document Analysis, Cyber Capabilities.

1. Introducción

La Ciberseguridad es identificada como "las tecnologías, los procesos y las políticas que ayudan a prevenir y/o reducir el impacto negativo de los eventos en el ciberespacio que pueden ocurrir como resultado de acciones deliberadas contra la tecnología de la

información por parte de un actor hostil o malintencionado" (Clark – Berson y Lin, 2014). Los ataques cibernéticos también han ido en aumento durante años anteriores a la pandemia de Covid-19, pero la cuarentena, las condiciones de vida cambiantes de los ciudadanos y las restricciones de viaje, aumentaron los ataques cibernéticos contra las naciones a medida que los ciudadanos dependían más de los servicios en línea. En el estudio de Buzzio-Garcia y coautores (2022), se afirma que, aunque América Latina sufrió más de 41 mil millones de ataques cibernéticos en 2020, la preparación cibernética para las empresas aún se encuentra en una fase inicial. Las tendencias negativas han sido percibidas por los ciudadanos a través de una encuesta (Marsh-McLennan, 2020) en la que el 31% de los encuestados afirmó que hubo un aumento en el número de ciberataques. Por su parte, las empresas han detectado ataques de ingeniería social (phishing) y malware, la mayoría de las veces dentro de la misma encuesta. En su artículo, Buzzio-Garcia y coautores resumieron casos específicos, incluidos phishing, ataques web y filtraciones de datos.

Basados en estos números, es importante examinar las interpretaciones de cómo los gobiernos centrales de los estados tienden a combatir el ciberdelito. Paralelamente, este artículo tiene como objetivo comparar las estrategias nacionales de ciberseguridad tanto desde el punto de vista cuantitativo como cualitativo de seis países latinoamericanos: Argentina, Brasil, Chile, Colombia, México y Perú. Los principales objetivos del estudio son investigar las últimas tendencias en el sector de la ciberseguridad en la región seleccionada y realizar un análisis comparativo basado en datos empíricos de estos países. La relevancia del tema se justifica por el creciente número de ciberataques, mientras en un momento en el cual la región latinoamericana aún se encuentra en la fase inicial de manejo de la política cibernética. Sin embargo, dichos países emergentes tienen un alto potencial de desarrollo futuro en este ámbito.

El artículo está dividido en seis secciones. Después de la introducción, el segundo capítulo revisa la literatura actual sobre política y estrategia cibernética latinoamericana. La metodología se describe en la tercera sección, seguida de una descripción general de la preparación cibernética de la región en la cuarta sección. En la quinta parte se presenta el análisis comparativo, mientras que en la sección final se exponen las conclusiones.

2. El rol de las estrategias de ciberseguridad en el desarrollo de las capacidades cibernéticas

Para los mercados emergentes, la conformación social y cultural en la creación de capacidad de seguridad cibernética y la creación de una conciencia cibernética, pueden ser una forma efectiva y a la vez rentable de fortalecer la inmunidad de la nación en el ciberespacio (Creese et al., 2021). Sin embargo, esta no es una solución suficiente en términos del desarrollo de capacidades cibernéticas nacionales que requiere una visión estratégica armonizada (Solar, 2020). Aquí aparece la noción de "gobernanza de la ciberseguridad" refiriéndose a "una visión holística e integrada de la seguridad de las

redes, sistemas, servicios e infraestructuras en la sociedad. Dicha noción de gobernanza incluye las instituciones, iniciativas políticas, programas y otros mecanismos (formales e informales) que forman parte de un ecosistema de capacidades y responsabilidades distribuidas en materia de ciberseguridad" (Hurel, 2021). Ahora bien, la estrategia nacional de ciberseguridad resulta fundamental para que un país unifique sus capacidades cibernéticas. Como elemento de la estrategia, la gobernanza de ciberseguridad apareció por primera vez en la Estrategia E-Ciber de Brasil en 2020.

> [...] La estrategia de ciberseguridad puede ser considerada como manifestaciones políticas del país suscriptor en la medida en que su contenido tienda a dividir responsabilidades entre los actores nacionales, estipular los objetivos estratégicos que se persiguen, definir las metas, pasos concretos a alcanzar en plazos definidos, e identificar las amenazas potenciales percibidas por el país [...] (Luiijf et al, 2013).

Además del nivel nacional, la región es activa en iniciativas internacionales de ciberseguridad, mostrando madurez en términos de aspectos culturales y sociales. Los países participan en la plataforma CSIRT (Computer Security Incident Response Team) Américas, dentro de un marco colaborativo, y también en los programas de ciberseguridad de la Organización de los Estados Americanos (OEA). La OEA prestó apoyó a los siguientes países para emitir sus primeras estrategias de ciberseguridad: Colombia (2011 y 2016), Chile (2017), México (2017) y Brasil (2018 y 2020) (Contreras - Barrett, 2020). Es importante señalar que la militarización del ciberespacio genera el peligro de que los países utilicen sus capacidades en esta área conduciendo a la "caracterización del entorno digital como un dominio 'cibernético' marcial" (Zittrain, 2017: 301). En este sentido, durante el 2016, la OTAN reconoció el ciberespacio como ámbito de las operaciones militares (Brent, 2019). En su trabajo, Tikk y Kertutunen (2020) establecieron cuatro posibles narrativas de la seguridad cibernética internacional: "la suma de todos los temores de seguridad cibernética global, una combinación de preocupaciones de seguridad cibernética nacional o estrictamente una cuestión de paz o guerra".

En consonancia con los autores en mención, Izycki (2018) realizó un análisis comparativo de las estrategias de ciberseguridad, señalando los objetivos de documentos, entre los que se encuentran como: la protección de infraestructuras críticas, la educación y formación, la protección de datos y el marco regulatorio, entre otros. Además, Kosevich (2020) presentó algunas de estas estrategias dibujando perfiles de países.

3. Metodología

La metodología utilizada en el presente artículo cuenta con un enfoque mixto en la medida que se han realizado análisis cuantitativos y cualitativos. El análisis cuantitativo se puede dividir en dos partes. Bolgov (2020) sugiere que una forma de evaluar la eficacia

de las políticas es comparar las posiciones de los países en las clasificaciones mundiales. En primer lugar, los indicadores básicos introdujeron una imagen general de los países seleccionados, incluidos indicadores específicos individuales y a nivel de país. Estos se pueden encontrar en la sección de descripción general del estudio. Luego, se realizó un análisis cuantitativo más detallado utilizando el Índice Nacional de Ciberseguridad (National Cyber Security Index o NCSI, en inglés). El Índice Nacional de Ciberseguridad es un índice global que mide la preparación de los países para prevenir amenazas cibernéticas y gestionar incidentes cibernéticos. El NCSI también es una base de datos con materiales de evidencia disponibles públicamente y una herramienta para el desarrollo de capacidades nacionales en ciberseguridad. El proceso de desarrollo del NCSI se puede determinar en cinco pasos:

1. Identificación de amenazas cibernéticas a nivel nacional
2. Identificación de medidas y capacidades de ciberseguridad
3. Selección de aspectos importantes y medibles
4. Desarrollo de indicadores de ciberseguridad
5. Agrupación de indicadores de ciberseguridad

La base de datos se centra en los aspectos medibles de la ciberseguridad implementados por los gobiernos centrales nacionales, incluidas las legislaciones vigentes, las unidades establecidas, los formatos de cooperación y los resultados. Recoge evidencias en tres categorías, 12 capacidades y 46 indicadores. Los países acumulan puntos basados en las evidencias de la siguiente manera:

- 1 punto: un acto legal que regula un área específica
- 2-3 puntos: una unidad especializada
- 2 puntos: un formato de cooperación oficial
- 1 a 3 puntos: un resultado/producto

La base de datos contiene datos específicos de cada país sobre Argentina (25 de junio de 2019), Brasil (24 de septiembre de 2019), Chile (3 de diciembre de 2020), Colombia (13 de febrero de 2019), México (25 de enero de 2021) y Perú (28 de agosto 2019). El valor de la base de datos se puede encontrar en los datos mundiales fáciles de comparar y las evidencias recopiladas para cada indicador. Cabe señalar que las legislaciones citadas se pueden encontrar en la base de datos del NCSI con enlaces que apuntan a los documentos originales, razón por la cual no se incluyen en la lista de referencia.

Para el análisis cualitativo se realizó un análisis cualitativo de contenido sobre las estrategias nacionales de ciberseguridad. Estas estrategias fueron recopiladas del Repositorio Nacional de Estrategias de Ciberseguridad recopiladas por la Unión Internacional de Telecomunicaciones. Las siguientes estrategias estuvieron involucradas en el análisis:

- Argentina: Estrategia Nacional de Ciberseguridad de la República Argentina (2019)
- Brasil: Estratégia Nacional de Segurança Cibernética (E-Ciber) (2020)
- Chile: Política Nacional de Ciberseguridad (PNCS) 2017–2022 (2017)
- Colombia: Política Nacional de Seguridad Digital (2016)
- México: Estrategia Nacional de Ciberseguridad (2017)
- Perú: en proceso

Es importante señalar que Perú aún no ha emitido su estrategia nacional de ciberseguridad, pero su política cibernética es competitiva en relación con los otros países estudiados.

4. Visión general de la región latinoamericana en términos de preparación digital

Antes de analizar las estrategias nacionales de ciberseguridad de los países latinoamericanos elegidos que participan en la comparación, es fundamental dar una visión general de la situación actual de estos estados. Por lo tanto, esta sección describe las condiciones generales de dichos países en términos de preparación digital, incluyendo datos tanto a nivel individual como nacional que utilizan diferentes indicadores básicos. Los datos aquí utilizados fueron accedidos desde bases de datos de código abierto que están disponibles en línea, con un enfoque en la elección de los últimos datos relevantes disponibles en el caso de cada estado.

Para conocer mejor las estrategias nacionales de ciberseguridad y qué causas y procesos legales, políticos, económicos o sociales están detrás de ellas, es importante observar las condiciones generales de estos países en base a varios indicadores. Primero, vale la pena compararlos según el Índice de Desarrollo Humano (IDH) que consta de tres pilares que incluyen la esperanza de vida, el índice de educación y el índice de ingreso nacional bruto (INB). En cuanto al IDH, Chile ocupa la primera posición ubicándose en el lugar 43 a nivel mundial (0,851 puntos), seguido de Argentina (lugar 46), México (lugar 74), Perú (lugar 79), Colombia (lugar 83) y Brasil (lugar 84). Sin embargo, el índice IDH mide el desarrollo humano en términos generales, por lo que, para obtener una mejor comprensión, se deben considerar otros indicadores estrechamente relacionados con los dispositivos digitales.

El Índice de Competitividad Digital Mundial de IMD (Institute for Management Development, en inglés), de Lausanne – Suiza, mide la preparación del país en base a tres pilares, incluidos el conocimiento, la tecnología y la preparación para el futuro. El informe de 2021 muestra que los países con mejor desempeño son los que ocupan un lugar más alto en el pilar de preparación para el futuro, lo que destaca la importancia de la capacidad de un estado para adaptarse a un entorno que cambia rápidamente. Al respecto, Chile domina, ubicándose en el lugar 39, seguido de Brasil (lugar 51), México (lugar 56), Perú (lugar 57), Colombia (lugar 59) y Argentina (lugar 61). Al estudiar los pilares constitutivos,

podemos ver que la mayoría de los países estudiados ocupan los primeros lugares en el pilar de tecnología, mientras que Chile y Perú se destacan en el pilar de conocimiento.

También vale la pena estudiar la clasificación de la Unión Internacional de Telecomunicaciones (UIT Clasificación) que trata sobre el uso general de Internet y la proporción de penetración de Internet en la sociedad. La proporción de individuos que utilizan Internet en comparación con el conjunto de la sociedad muestra datos interesantes. Al respecto, Argentina se destaca con un 85%, seguida de Chile (82%), Brasil (74%), México (72%) y Colombia y Perú, ambos con 65-65%. Al desglosar la proporción de usuarios de Internet por grupos de edad, podemos ver diferencias significativas. El grupo de edad más activo es el de 15 a 24 años, con un 92% en Brasil y México, un 90% en Argentina, un 84% en Colombia y un 83% en Perú. Es interesante ver una proporción relativamente alta de usuarios de Internet entre el grupo de edad de más de 75 años en Brasil (83%), México (68%) y Colombia (60%). En cuanto a las habilidades digitales (donde hay datos disponibles), solo el 20-31% de la sociedad tiene habilidades básicas, mientras que un porcentaje mucho más bajo, entre el 2-12% del total, tiene habilidades avanzadas. Estos datos destacan sin embargo que, a medida que la infraestructura tecnológica se desarrolla en los países estudiados, los ciudadanos no pueden seguir el ritmo de estas mejoras. Lo anterior genera una presión sobre la sociedad que hace que las personas sin las suficientes habilidades digitales estén expuestas a ciberataques y sean vulnerables dentro de su "vida digital".

Después de obtener la imagen de las capacidades digitales individuales de las poblaciones en los países estudiados, vale la pena tener una idea del mercado digital e Internet de América Latina. El valor del cibermercado en esta región muestra una tendencia dinámicamente creciente entre 2019 y lo proyectado para el 2025. En 2019 tenía un valor de 12.880 millones de dólares; en 2022 17.780 millones de USD y se prevén un total de 26.200 millones de USD para el 2025 (Statista, 2021). Sin embargo, esta tendencia creciente está muy expuesta a ciberataques que provocan daños que pueden ser medidos en el coste medio de las filtraciones de datos. Observando los datos de 2020, América Latina (1,68 millones de dólares) está rezagada con respecto a otras regiones y países del mundo, por ejemplo, respecto al líder mundial Estados Unidos (8,64 millones de dólares), Medio Oriente (6,52 millones de dólares) o Canadá (4,5 millones de dólares). Por otro lado, Brasil es el 13º país de la lista con 1,12 millones de dólares.

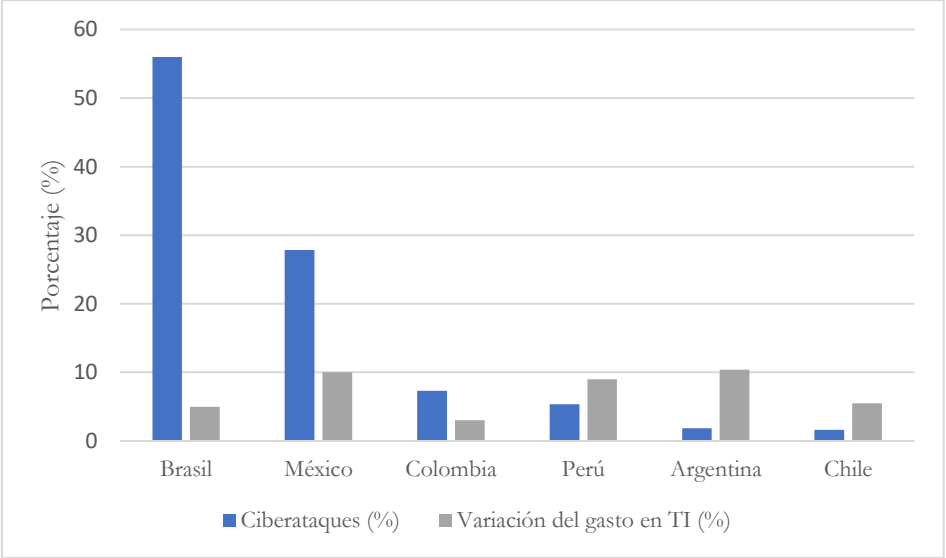

Figura 1. Proporción de ciberataques (en %) y variación en el gasto en TI (en %)
(Fuente: Contribución propia de los autores basada en datos de Statista (2022))

En la Figura 1. se resumen la proporción de ataques cibernéticos entre los países de América Latina (basado en datos de 2020) y la variación en el gasto en tecnología de la información (TI) (basado en datos de 2021). En este punto debiéramos esperar que el país más expuesto en términos del número de ciberataques se enfoque más en su TI, pero como se puede advertir en la figura, este no es el caso. La mayoría de los ciberataques fueron dirigidos a Brasil en 2020 (55,97%), seguido de México (27,86%) y Colombia (7,33%). Mientras que la mayor variación del gasto en TI en 2021 se dio en Argentina (10,4%), seguida de México (10%) y Perú (9%) (Statista, 2022), esto puede ser una señal de advertencia para Brasil. El sector público está aún más expuesto ya que la mayoría de las infraestructuras críticas del país están a cargo de este sector. Los datos de 2019 muestran los ataques a aplicaciones web en el sector público, nuevamente están dominados por Brasil con 27.900 ataques, seguido de Colombia (10.006 ataques), Argentina (3.606 ataques), México (1.716 ataques), Perú (256 ataques) y Chile (54 ataques) (Statista, 2021).

5. Análisis de la estrategia de ciberseguridad

El marco de este estudio no brinda el suficiente espacio para elaborar en detalle los diferentes aspectos incluidos en el Índice Nacional de Ciberseguridad y el Índice de Desarrollo Digital. Sin embargo, se pueden observar el total de puntos alcanzados resumidos en la Figura 2.

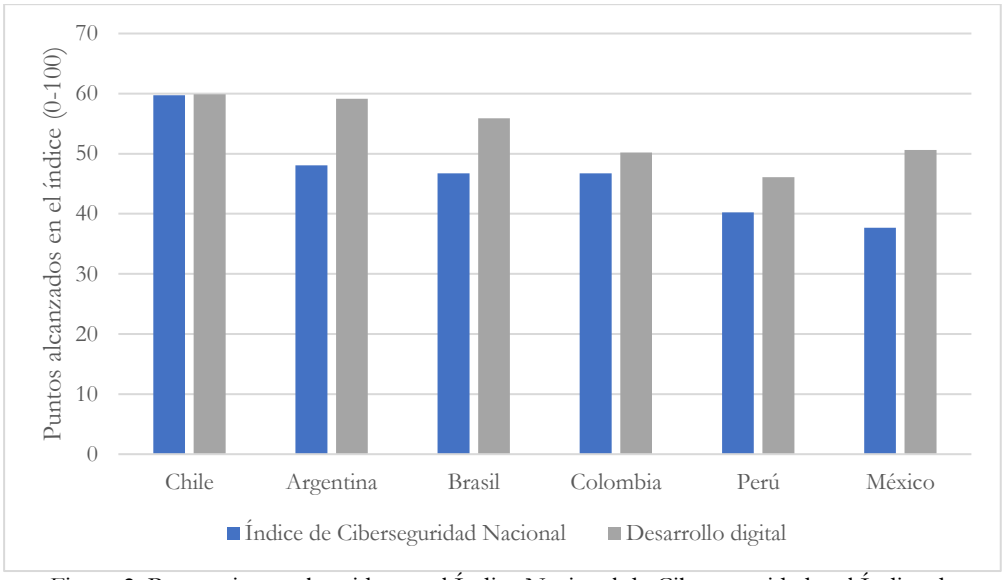

Figura 2. Puntuaciones obtenidas en el Índice Nacional de Ciberseguridad y el Índice de Desarrollo Digital (Fuente: Contribución propia de los autores basada en datos del NCSI (NCSI.ega.ee))

En base al total de puntos alcanzados por los países en el NCSI, Chile domina con 59,74 puntos, seguido de Argentina (48,05) y Brasil (46,75). El Índice de Desarrollo Digital muestra una clasificación algo similar entre los países, con la posición de liderazgo aún en manos de Chile (59,88), seguido de Argentina (59,13) y Brasil (55,89). Sin embargo, podemos ver que, en base al NCSI, Colombia ocupa el 4° lugar entre los países estudiados, mientras que, con base en el Desarrollo Digital, México ocupa el 4° lugar. En el ranking mundial se encuentran los siguientes puestos: Chile en el puesto 47, Argentina en el 71, Colombia en el 74, Brasil en el 75, Perú en el 81 y México en el 84 (NCSI, 2022). Es interesante que, a pesar de aún no haber emitido su propia estrategia nacional, Perú está mejor clasificado en base a su política de medidas que México. Si profundizamos en los diferentes aspectos del índice, podemos determinar el nivel de madurez de cada país.

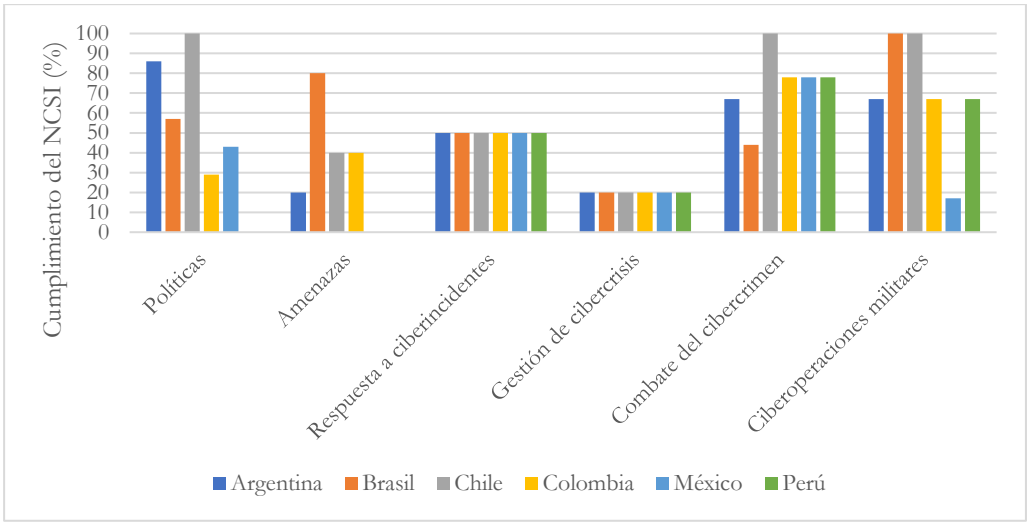

Figura 3. Puntajes obtenidos en indicadores relacionados con la política y la defensa del Índice Nacional de Ciberseguridad (Fuente: Contribución propia de los autores basada en datos del NCSI (NCSI.ega.ee))

El primer conjunto de indicadores está relacionado más bien con las dimensiones políticas y de defensa de la ciberseguridad, y la política de ciberseguridad en general (Figura 3). Entre estas, la respuesta a los ciberincidentes y la gestión de las cibercrisis son las que ninguno de los países alcanzó el nivel de preparación total. Todos los países estudiados establecieron una unidad de respuesta a incidentes cibernéticos. Se pueden encontrar datos sobre el establecimiento del CERT (Centro de Respuesta a Incidentes Cibernéticos de México) siendo el 1 de junio de 2010, mientras que, en Chile, la Resolución Exenta N 5.006 de agosto de 2019 creó las unidades gubernamentales especializadas en ciberseguridad, incluido el Departamento CSIRT. En Brasil también operan unidades CSIRT (en inglés: computer security incident response team) y CERT (en inglés: computer emergency response team), mientras que en Colombia y Perú podemos encontrar unidades CERT. En cuanto a la lucha contra el delito cibernético, Chile domina, ya que los delitos cibernéticos están tipificados, con una unidad de delitos cibernéticos una unidad de análisis forense digital y un punto de contacto 24/7 para delitos cibernéticos internacionales.

Es importante señalar que todos los países penalizan el delito cibernético en su legislación nacional. El primer Estado en tener un acto legal fue Argentina dentro de su Ley N° 26.388 del 24 de junio de 2008, que modifica el Código Penal y define diferentes tipos de delitos cibernéticos que incluyen la interceptación de comunicaciones, obtener acceso ilícito a sistemas informáticos, causar daño a dichos sistemas informáticos, fraude, falsificación electrónica o documentos basados en TI, interrumpir comunicaciones y borrar o alterar evidencia digital. En cuanto al análisis de amenazas, Brasil se destaca por

tener una unidad de análisis de amenazas y proporcionar un sitio web de ciberseguridad administrado por una autoridad pública. Brasil tiene dos sitios web relacionados; uno es la "Guía de seguridad en Internet" a cargo de la unidad CERT y el Comité Directivo de Internet de Brasil, mientras que el otro es un sitio web dirigido a niños y adolescentes sobre contenido relacionado con la seguridad cibernética.

Brasil y Chile lideran las operaciones cibernéticas militares, cuentan con unidades de operaciones cibernéticas y realizan con éxito ejercicios de operaciones cibernéticas. Cabe señalar que todos los países estudiados ya han participado en ejercicios de operaciones cibernéticas internacionales: Argentina y Chile estuvieron en la operación Panamax 2016, mientras que los demás países se sumaron más tarde a la operación Panamax 2018. En general, el aspecto de formulación de políticas está más desarrollado en Chile, seguido por Argentina. La primera unidad de políticas de ciberseguridad fue establecida en Chile por el Decreto Supremo Nº 533/2015, que creó un Comité Interministerial de Ciberseguridad (CICS). Posteriormente, el Decreto Supremo Nº 579/2019 modificó esto, creando una nueva comisión técnica con facultades consultivas en materia de ciberseguridad. Los otros dos países donde operan unidades de política de ciberseguridad son Argentina (Dirección Nacional de Ciberseguridad creada por el Jefe de Gabinete, DA 103/2019) y Brasil (Departamento de Seguridad de la Información creado por el Decreto 9668 de 2019).

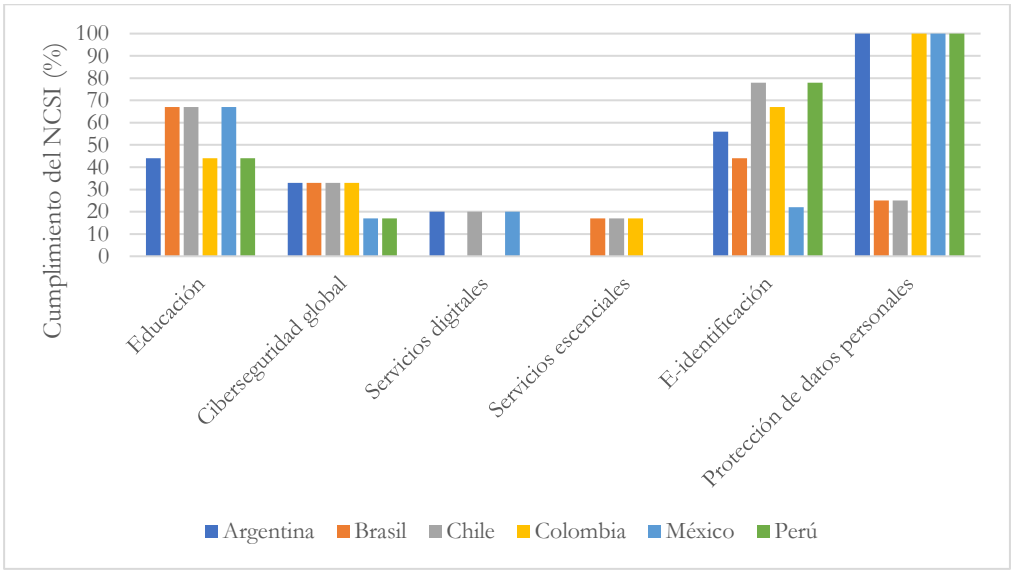

Figura 4. Puntajes obtenidos en indicadores relacionados con servicios y protección de datos del Índice Nacional de Ciberseguridad (Fuente: Contribución propia de los autores basada en datos del NCSI (NCSI.ega.ee))

El segundo conjunto de indicadores está relacionado principalmente con temas de servicios y protección de datos (Figura 4). Podemos ver una tendencia general a la baja en cada país en estos aspectos de la política de ciberseguridad, excepto la protección de datos personales, que alcanza un nivel de preparación total en Argentina, Colombia, México y Perú. En cuanto a la protección de los servicios digitales y servicios esenciales, algunos países aún no han implementado ninguna política (mientras que el primero está ausente en Brasil, Colombia y Perú, el segundo está ausente en Argentina, México y Perú). En materia de protección de servicios digitales, Argentina, Chile y México se destacan como emisores de estándares de ciberseguridad para el sector público. En Argentina se ha establecido un Modelo de Política de Seguridad de la Información para las autoridades públicas; en Chile, la Orden Presidencial Nº 8, 2018 de Ciberseguridad implementa estas medidas específicas, mientras que, en México, la Guía de Ciberseguridad para Instalaciones Públicas se emitió en 2018. En relación con la educación en ciberseguridad, la mayoría de los países ofrecen títulos de ciberseguridad a nivel de licenciatura y maestría, pero ninguno de ellos tiene títulos de nivel de doctorado. En cuanto a la contribución a la ciberseguridad global, podemos ver una baja tendencia general en cada país, estando en la fase inicial de la cooperación internacional como nuevas potencias cibernéticas emergentes. Aunque está en una fase inicial, la primera contribución se ha realizado por parte de cada país, ya que todos son miembros de la Red de las Américas del CSIRT, el Foro de Equipos de Seguridad y Respuesta a Incidentes (FIRST) y la Unión Internacional de Telecomunicaciones (UIT). La protección de datos personales está bien elaborada, con legislación a nivel nacional y una autoridad de protección de datos personales también.

Además del análisis cuantitativo basado en índices, es crucial realizar un análisis de contenido cualitativo de las estrategias nacionales de ciberseguridad de los países elegidos. Como ya se ha mencionado, Perú aún no ha emitido una estrategia nacional de ciberseguridad; sin embargo, como se reflejó en el análisis basado en índices, el país ya ha implementado varias de las medidas esenciales en su política de seguridad cibernética. Dentro del análisis cualitativo se comparan las estrategias en base a cinco dimensiones. Estas dimensiones están relacionadas con los objetivos determinados por los gobiernos nacionales, entre ellos: la educación en ciberseguridad, las medidas relacionadas con la detección de incidentes cibernéticos, la regulación de la ciberseguridad, la cooperación internacional con otros estados y la colaboración con actores industriales.

País	Argentina	Brasil	Chile	Colombia	México
Educación	X		X		X
Detección	X	X	X	X	X
Regulación	X		X	X	
Cooperación internacional	X	X	X	X	X
Cooperación industrial	X		X		

Tabla 1. Resultados del análisis cualitativo de la estrategia entre cinco dimensiones (Fuente: elaboración propia en base de la estrategia nacional de cada país)

La Tabla 1 resume si las dimensiones mencionadas anteriormente están incluidas en las estrategias nacionales de ciberseguridad, revelando sobre su complejidad. Entre los países estudiados, Argentina y Chile incluyeron todos los factores, mientras que Colombia y México incluyeron solo 3, seguidos por Brasil que incluye 2 de ellos. Si observamos los factores, es importante notar que la detección y la cooperación internacional están presentes en cada estrategia, mientras que la educación en solo 3, la regulación y la cooperación industrial están presentes solo en 2 estrategias.

La complejidad de las estrategias nacionales basadas en estos factores se encuentra en paralelo con los resultados del NCSI, ya que Chile y Argentina dominan a los demás países estudiados en el ranking mundial. En cuanto a las acciones articuladas en la estrategia, se pueden identificar perfiles de los países.

Argentina definió la educación en ciberseguridad creando un plan nacional de concientización sobre seguridad en el ciberespacio, promoviendo la formación de profesionales, técnicos e investigadores en el campo de la ciberseguridad. Además de la educación, la promoción de la industria cibernética juega un papel clave.

Brasil en su estrategia nacional de ciberseguridad la aborda con un enfoque del sector público. Las acciones también están relacionadas principalmente con el sector público, incluida la celebración de foros de gobernanza y el establecimiento de requisitos mínimos de ciberseguridad en los contratos de los organismos públicos. El aspecto de defensa también se enfatiza en la estrategia al promover el análisis conjunto contra los ciberdelitos y fomentar el intercambio de información sobre ciberincidentes y vulnerabilidades.

Chile expresa una fuerte voluntad de cooperación internacional en su estrategia, incluyendo la política cibernética dentro de la política exterior chilena, y promueve normativas internacionales que fomentan la confianza y la seguridad en el ciberespacio.

Colombia identifica la infraestructura cibernética como infraestructura crítica y promueve una estrategia de defensa de las mismas. La estrategia además de este enfoque es la ciberseguridad desde el lado de la gestión de incidentes y el análisis forense digital, mencionando los delitos cibernéticos.

México también pone énfasis en la prevención del delito cibernético, sin embargo, su enfoque es muy amplio, mencionando objetivos y acciones más generales como el desarrollo de una cultura de ciberseguridad, el desarrollo de capacidades cibernéticas y el desarrollo del marco legal y la autorregulación.

6. Conclusión

Con el creciente número de ataques cibernéticos y la importancia cada vez mayor del ciberespacio en el desarrollo de capacidades internacionales y nacionales, es más importante que nunca elaborar estrategias nacionales y establecer unidades que se ocupen de los problemas relacionados con ciberseguridad. Los mercados emergentes están rezagados con respecto a los estados más desarrollados, pero la voluntad de desarrollar políticas cibernéticas se refleja en las tendencias de los últimos años. Los estados

latinoamericanos, están más que nunca comprometidos con fortalecer la conciencia social y cultural en el dominio cibernético y a cooperar regionalmente para mejorar sus capacidades y compartir información y mejores prácticas. Estas tendencias resaltan la relevancia de estudiar las estrategias de ciberseguridad desde un enfoque comparativo.

Este estudio tuvo como objetivo medir el nivel de madurez de seis países latinoamericanos, Argentina, Brasil, Chile, Colombia, México y Perú, a partir de indicadores básicos que permiten conocer sobre su preparación digital y el comportamiento de los usuarios de Internet, y también, más específicamente, a partir de sus estrategias nacionales de ciberseguridad. El análisis comparativo se realizó tanto desde un aspecto cuantitativo basado en los datos del Índice Nacional de Seguridad Cibernética, que es una base de datos global y un sistema de clasificación, como desde un aspecto cualitativo mediante el análisis de contenido. Ciertas consecuencias pueden extraerse después del análisis. En primer lugar, estos países están muy expuestos a los ataques cibernéticos por parte de un número cada vez mayor de usuarios de Internet y de redes sociales, y debido a que cuentan con un marco institucional, de infraestructura y regulatorio, que no está lo suficientemente preparado. Es importante señalar que la mayoría de los ciberataques están dirigidos contra Brasil; esto no se refleja en el gasto del país en tecnología de información (TI).

Analizando los datos nacionales basados en el NCSI y el Índice de Desarrollo Digital, Chile se destaca en general; sin embargo, el país aún se encuentra en la fase inicial en materia de protección digital y de servicios esenciales, protección de datos personales y gestión de cibercrisis. La posición de Brasil es interesante, ubicándose en el 3er lugar general, siendo el país más atacado por ciberataques en la región. Brasil se destaca en términos de análisis de amenazas y operaciones cibernéticas militares. Basado en el análisis de contenido, pudimos apreciar que Chile y Argentina, que también lideran el ranking de NCSI, tienen una estrategia de seguridad cibernética más holística, que incluye factores como la educación en seguridad cibernética, la detección de delitos cibernéticos, el marco regulatorio y el objetivo de cooperar con socios industriales e internacionales.

Para concluir, estos países se encuentran en la fase inicial en cuanto al nivel de eficiencia de sus estrategias nacionales de ciberseguridad; en muchos casos, incluso el plan de implementación está ausente. Por otro lado, tienen un enorme potencial para un mayor desarrollo. Los gobiernos centrales afirman su intención y eventos recientes como la pandemia de Covid-19 resaltan la necesidad de estas estrategias coordinadas.

Referencias bibliográficas

Bolgov, Radomir (2020). The UN and Cybersecurity Policy of Latin American Countries. *2020 Seventh International Conference on eDemocracy eGovernment, (ICEDEG*). 259-263. DOI: 10.1109/ICEDEG48599.2020.9096798

Brent, Laura (2019). NATO's role in cyberspace. *NATO Review*. Asequible en: https://www.nato.int/docu/review/articles/2019/02/12/natos-role-in-cyberspace/index.html, fecha de consulta: 03-05-2022.

Clark, David – Berson, Thomas – Lin, Herbert S. (eds.) (2014). *Computer Science and Telecommunications Board, At the Nexus of Cybersecurity and Public Policy*. Washington DC: The National Academy Press.

Creese, Sadie – Dutton, William H. – Esteve-González, Patricia (2021). The social and cultural shaping of cybersecurity capacity building: a comparative study of nations and regions. *Pers Ubiquit Comput,* 25. 941–955. DOI: 10.1007/s00779-021-01569-6

Contreras, Belisario – Barrett, Kerry-Ann (2020). Challenges in building regional capacities in cybersecurity: A regional organizational reflection. *Routledge handbook of international cybersecurity*. 214-217. DOI: 10.4324/9781351038904-20

Estado del Riesgo Cibernético en Latinoamérica en tiempos de COVID-19 (2020). Marsh & McLennan Company.

Buzzio-Garcia, Jorge – Salazar-Vilchez. Victor – Moreno-Torres, Jhonatan – Leon-Estofanero, Omar (2021). Review of Cybersecurity in LatinAmerica during the Covid-19 Pandemic. A brief Overview, *IEEE Fifth Ecuador Technical Chapters Meeting (ETCM)*, 1-5. DOI: 10.1109/ETCM53643.2021.9590693

Hurel, Louise Marie (2021). Cybersecurity in Brazil: an analysis of the National Strategy. Asequible en: https://igarape.org.br/en/cybersecurity-in-brazil-an-analysis-of-the-national-strategy/, fecha de consulta: 03-05-2022.

Izycki, Eduardo (2018). National cyber security strategies in Latin America: Opportunities for convergence of interests and consensus building. *RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação,* (E15). 39-52.

Kosevich, Ekaterina (2020). Estrategias de seguridad cibernética en los países de América Latina. *Iberoamérica,* 1. 137-159. DOI: 10.37656/S20768400-2020-1-07

Luiijf, Eric – Besseling, Kim – De Graaf, Patric (2013). Nineteen national cyber security strategies. *International Journal of Critical Infrastructure Protection,* 9(1-2). 3-31.

Solar, Carlos (2020). Cybersecurity and cyber defence in the emerging democracies. *Journal of Cyber Policy,* 5(3). 392-412. DOI: 10.1080/23738871.2020.1820546

Tikk, Eneken – Kerttunen, Mika (2020). Introduction. En: Tikk, Eneken – Kerttunen, Mika (eds). *Routledge Handbook of International Cybersecurity*. 1-8. New York: Routledge. DOI: 10.4324/9781351038904

Zittrain, Jonathan (2017). "Netwar": The Unwelcome Militarization of the Internet has Arrived. *Bulletin of the Atomic Scientists,* 73(5). 300-304. DOI: 10.1080/00963402. 2017.1362907

Artículos publicados en internet

CSIRT Americas platform. Asequible en: https://cybilportal.org/projects/americas-csirt-network-and-virtual-platform/, fecha de consulta: 05-05-2022.

Decreto Supremo 533 de 2015 [Ministerio del Interior y Seguridad Pública]. Por el cual, se crea comité interministerial sobre ciberseguridad. 17 de Julio de 2015. Asequible en: https://www.bcn.cl/leychile/navegar?i=1079608, fecha de consulta: 05-05-2022.

Decreto Supremo 9.668 de 2019. Poder Executivo. Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Funções de Confiança do Gabinete de Segurança Institucional da Presidência da República e altera o quantitativo de Gratificações de Exercício de Cargo em Confiança devida a Militares - RMP. 2 de Enero de 2019. Asequible en: https://www2.camara.leg.br/legin/fed/decret/2019 /decreto-9668-2-janeiro-2019-787575-norma-pe.html, fecha de consulta: 05-05-2022.

Decreto Supremo 579 de 2019 [Ministerio del Interior y Seguridad Pública]. Por el cual, se modifica el Decreto Supremo 533 de 2015, que crea comité interministerial sobre ciberseguridad. 6 de noviembre de 2019. Asequible en: http://bcn.cl/2hgau fecha de consulta: 05-05-2022.

Dirección Nacional de Ciberseguridad creada por el Jefe de Gabinete, DA 103/2019. Asequible en: http://servicios.infoleg.gob.ar/infolegInternet/anexos/320000-324999 /320081/norma.htm, fecha de consulta: 05-05-2022.

Estrategia Nacional de Ciberseguridad de la República Argentina (2019). Asequible en: https://www.argentina.gob.ar/normativa/323594_res829-01_pdf/archivo, fecha de consulta: 05-05-2022.

Estratégia Nacional de Segurança Cibernética (E-Ciber) (2020). Asequible en: https://www.gov.br/governodigital/pt-br/estrategias-e-politicas-digitais/estrategia-nacional-de-seguranca-cibernetica, fecha de consulta: 05-05-2022.

Política Nacional de Ciberseguridad (PNCS) 2017–2022 (2017). Asequible en: https://www.unodc.org/e4j/data/_university_uni_/chiles_national_cybersecurity_policy_2017-2022.html?lng=en, fecha de consulta: 05-05-2022.

National Cybersecurity Strategy (2017). Asequible en: https://www.gob.mx/cms /uploads/attachment/file/399655/ENCS.ENG.final.pdf, fecha de consulta: 03-05-2022.

Política Nacional de Seguridad Digital (2016). Asequible en: https://colaboracion. dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf, fecha de consulta: 03-05-2022.

Organization of the American States list of members. Asequible en: https://www.oas.org/en/member_states/default.asp, fecha de consulta: 03-05-2022.

Bases de datos

Índice de Desarrollo Humano (IDH). Asequible en: https://hdr.undp.org/en /content/download-data, fecha de consulta: 04-05-2022.

Índice de Competitividad Digital Mundial (IMD). Asequible en: https://www.imd.org /centers/world-competitiveness-center/rankings/world-digital-competitiveness/, fecha de consulta: 04-05-2022.

Unión Internacional de Telecomunicaciones (UIT) Clasificación. Asequible en: https://www.itu.int/en/ITU-D/Statistics/Pages/facts/default.aspx, fecha de consulta: 04-05-2022.

NCSI - National Cybersecurity Index. Asequible en: https://ncsi.ega.ee/ncsi-index/, fecha de consulta: 03-05-2022.

Repositorio Nacional de Estrategias de Ciberseguridad. Asequible en: https://www.itu.int /en/ITU-D/Cybersecurity/Pages/National-Strategies-repository.aspx, fecha de consulta: 03-05-2022.

Statista. Value of the cybersecurity market in Latin America in 2019 and 2025. Asequible en: https://www.statista.com/statistics/1180184/value-cybersecurity-market-latin-america/, fecha de consulta: 03-05-2022.

Statista. Average cost of data breaches worldwide as of 2020, by country or region (in million U.S. dollars). Asequible en: https://www.statista.com/statistics/463714/cost-data-breach-country/, fecha de consulta: 03-05-2022.

Statista. Countries in Latin America most targeted by cyber attacks in 2020. Asequible en: https://www.statista.com/statistics/818412/latin-american-countries-highest-share-cyber-attacks/, fecha de consulta: 03-05-2022.

Statista. Change in information technology (IT) spending in selected countries in Latin America in 2021. Asequible en: https://www.statista.com/statistics/1190544/latin-america-it-spending/, fecha de consulta: 03-05-2022.

Statista. Latin American countries with the largest number of web application attacks observed in the public sector in June 2019. Asequible en: https://www.statista.com /statistics/1066172/most-targeted-countries-web-application-attacks-public-sector-latin-america/, fecha de consulta: 03-05-2022.