Retos de América Latina para la construcción de una política nacional de ciberseguridad: una apuesta a 2030

Latin American challenges for the construction of a national cybersecurity policy: a bet to 2030

Por: **Juan Manuel Aguilar Antonio** 

Revista Académica Seguridad y Estrategia Año 2022. Volumen 1. Número 2. ISSN: 2790-1475

Fotografía propiedad de Ejército de Red de Conocimiento sobre Seguridad Ciudadana

Retos de América Latina para la construcción de una política nacional de ciberseguridad: una apuesta a 2030

Doctor en Ciencias Sociales
Juan Manuel Aguilar Antonio
Facultad de Ciencias Políticas y Sociales,
Universidad Nacional Autónoma de México
Conferencista del INEES
investigacionyposgrado@usjt.edu.mx

Recibido: 04-05-2022
Publicado: 15-12-2022

Resumen

La investigación aborda los retos de América Latina para el desarrollo de una Estrategia Nacional de Ciberseguridad (ENCS) para el 2030, frente al contexto global de ciberseguridad. El fin es crear una serie de recomendaciones frente a las debilidades, fortalezas, oportunidades y amenazas de la región. El texto se compone de tres partes, en la primera se presentan una conceptualización de qué es el ciber poder desde el poder del Estado-Nación. En el segundo, se presenta el contexto de ciber amenazas de América Latina y analizan sus capacidades cibernéticas. En la tercera sección, se presenta un análisis prospectivo para la construcción de escenarios futuros a 2030. Por último, se presentan unas breves conclusiones y recomendaciones.

Palabras Clave

- Seguridad Cibernética
- Seguridad Nacional
- Ciberpoder
- Capacidades Cibernéticas

Abstract

The research addresses the challenges of Latin America for the development of a National Cybersecurity Strategy (ENCS) for 2030, facing the global cybersecurity context. The purpose is to create a series of recommendations against the weaknesses, strengths, opportunities and threats of the region. The text is made up of three parts, in the first a conceptualization of what cyber power is from the power of the Nation-State is presented. In the second, the context of cyber threats in Latin America is presented and their cyber capabilities are analyzed. In the third section, a prospective analysis is presented for the construction of future scenarios to 2030. Finally, some brief conclusions and recommendations are presented.

Key Words

- Cybersecurity
- National security
- Cyber Power
- Cyber-capabilities

Revista Académica Seguridad y Estrategia Año 2022. Volumen 1. Número 2. ISSN: 2790-1475

Juan Manuel Aguilar Antonio

Introducción

La ciberseguridad es una parte trascendental de la política de seguridad nacional frente a un contexto adverso y cambiante de amenazas al Estado-Nación. También, desde una óptica prospectiva, también son una amenaza y riesgo latente para evitar la consolidación del futuro deseado por parte de los gobiernos de los países del mundo y sus Fuerzas Armadas.

En la actualidad, cada vez más amplia la brecha que existe entre las naciones líderes en el desarrollo de una Estrategia Nacional de Ciberseguridad (ENCS) y quienes carecen de una. Entre los países que han priorizado el desarrollo de la Inteligencia Artificial, Computación Cuántica, Redes 5G, o procesamiento de Big Data, que en largo plazo marcaran una clara divergencia entre los actores que se beneficien del ciberespacio y quienes estén al margen de él. La finalidad de este artículo es presentar una reflexión de dónde está situada América Latina en este contexto.

Ciberpoder: comprensiones desde el neorrealismo, teoría de la guerra y constructivismo

La emergencia del ciberespacio como nuevo dominio de la seguridad internacional supone su comprensión como una fuente de riesgos, amenazas a la sobrevivencia y búsqueda del futuro deseado por parte de los del Estado-Nación. Sobre este enfoque, Joshep Nye (2010) creó el término de ciberpoder al que definió como: "*la habilidad de obtener resultados privilegiados, crear ventajas, o influenciar en eventos a través del uso de recursos electrónicos interconectados en el ciber dominio*". Esta definición presenta al ciberespacio como una arena de interacción, pero también de control y manipulación, en que diversos actores pueden utilizar los recursos del internet y las TIC's a su disposición, para influir en la seguridad nacional, con el fin impactar en su estabilidad y/o modificar las condiciones de un gobierno.

En ese sentido, Sheldon (2012) expresa que el uso y aplicación del ciber poder está orientado en aspectos tácticos, técnicos y operacionales en el ciber dominio, lo cual, está influenciado por la creación de un objetivo estratégico por parte de los Estados-Nación, el cual se puede perseguir y tiene la función de manipular el contexto de un ambiente estratégico, para ganar algún tipo de superioridad por encima de los adversarios y degradar o limitar el desarrollo de capacidades de sus adversarios u oponentes, con lo cual el ciber poder es la suma de todos los efectos estratégicos generados por ciber operaciones en el mundo virtual.

Por su parte, Kuehl (2009) se refiere al concepto como: "*[el] centro de un conjunto nuevo de conceptos y doctrinas que son una palanca clave en el desarrollo y ejecución de política, ya sea contra el terrorismo, crecimiento económico o asuntos diplomáticos, etc.*" Mientras que para Starr (2012) es: *"[un instrumento] que a medida que evoluciona tiene el potencial de mejorar cada una de las palancas del poder nacional [de un Estado], en especial el militar y el informático"*.

En ese sentido, se destaca que la escuela teórica del neorrealismo ha dado un peso importante al análisis del ciberespacio como nueva esfera para ejercer el poder del Estado-Nación. Esta discusión empieza en 2010 con la publicación del artículo *Cyber Power* de Joseph Nye, en el que este autor expresó que la emergencia del ciberespacio como campo para ejercer poder se asocia a un proceso de difusión de poder en el siglo XXI. Esta difusión tiene nexos con la posesión o manipulación de información por parte de gobiernos nacionales, a través del internet, que les permitan garantizar seguridad y prosperidad (Nye, 2010).

También, los rápidos y vertiginosos avances de las Tecnologías de la Información y la Operación (TIC´s) y rápida reducción del costo del procesamiento y transmisión de información transformaron al ciberespacio en un nuevo dominio de protección para la soberanía, interés y seguridad nacional del Estado-Nación.

En este punto, es importante destacar que el análisis neorrealista resalta que el ciber poder no reemplaza al espacio geográfico y soberano de cada país. Sin embargo, acepta que éste es un régimen de componentes físicos y materiales que coexisten con el ejercicio del poder nacional y este debe ajustarse al control e influencia de la autoridad y leyes de los gobiernos de cada país (Choucri et al., 2013).

En este sentido, un elemento clave del neorrealismo es la consideración del papel vital de las empresas privadas, promotoras o creadores de software, como entidades de suma importancia para la consolidación de un régimen internacional de normas del internet, para salvaguardar la seguridad nacional.

Contexto de amenazas y capacidades cibernéticas de América Latina

Desde comienzos de la segunda década del siglo XXI, América Latina es una región en la cual las amenazas provenientes de ciberespacio han mostrado cada vez mayor complejidad para la seguridad nacional. El análisis sobre esta situación se inaugura con el informe Tendencias en la seguridad cibernética en América Latina y el Caribe y respuestas de los gobiernos de la Organización de los Estados Americanos y Symantec (2014), que expresa que desde 2012 los ciberataques a entidades o sitios de internet públicos y privados han crecido a cifras anuales de más del 61% en la región.

También, países como Ecuador, Guatemala, Bolivia, Perú y Brasil estuvieron dentro de los diez principales países que con más afectaciones por malware durante los años de 2014 a 2016. A la par que Uruguay, Colombia y Chile se posicionaron con cifras de infección por malware por encima de la media global, situación que enmarcó a la región junto a Asía, con las tasas más altas de virus maliciosos a nivel global (Aguilar-Antonio, 2019). Asimismo, es importante mencionar que desde 2015 el uso del ciberespacio para realizar fraude bancario se ha transformado en un problema, dado que la OEA (2018) estima que el 92% de las entidades financieras han presentado un ciber ataque, con una tasa de éxito del 37%.

En esta sintonía Kaspersky Lab (2020) registró más de 746 mil ataques de malware diarios durante el 2020 en América Latina, lo que implica que se realizan 9 ciber ataques de malware cada segundo. A la par que se detectó que los tres principales países con mayor incidencia para el ciber crimen son Brasil (56.25%, del total de la región), México (22.81%) y Colombia (10.20%). Del mismo modo, se debe citar que del total de 62 millones de ataques detectados por Kapersky en 2020, 66% se vinculaban a robo a entidades privadas y comerciales, mientras 34% restante se vinculaban a actividades criminales, hacktivismo y ataques a sistemas gubernamentales.

De esta forma, es necesario entender el contexto de capacidades cibernéticas de América Latina. Para esto, son de utilidad dos métricas internacionales que evalúan el nivel de desarrollo de los Estados-Nación, que son el Índice Nacional de Ciberseguridad o (National Cyber Security Index o NCSI en inglés), de la E- Governance Academy, y el Índice Global de Ciberseguridad (GCI por sus siglas en inglés), de la Unión Internacional de Telecomunicaciones. Este ejercicio se realiza a razón de que cada medición presenta las áreas de oportunidad y de mejora de las legislaciones nacionales contra ciber crimen, ENCS y consolidación de Equipos de Repuesta de Emergencia Informática (CERT), con el fin de mejorar las ciber capacidades de los países evaluados para garantizar su seguridad nacional y perseguir los intereses de su política exterior.

En sí, tanto el GCI (2018) y el NCSI (2019) sirven para brindar un diagnóstico de los países del mundo en materia de ciberseguridad. Asimismo, sirven para mostrar las asimetrías y la brecha en el desarrollo de ciber capacidades entre regiones como América Latina, África y Medio Oriente, y países que han priorizado el desarrollo de la ciberseguridad como las naciones de la OTAN.

Sobre el NCSI (2019) es importante mencionar que evalúa la preparación de los países para prevenir ciber amenazas y gestionar ciber incidentes como un ataque servicios esenciales e infraestructura nacional crítica, a través de doce indicadores, concentrados en una ponderación global

que van del 0 al 100, que permiten tener un diagnóstico de las capacidades de ciber defensa de los países evaluados.

Por su parte, el GCI (2018) mide el grado de compromiso e importancia que los Estados-Nación han dado al tema de la ciberseguridad en el desarrollo de su política de seguridad nacional. Con base en los cinco ejes de la Agenda Global de Ciberseguridad (AGCS), establecida por la ITU en 2007, vinculados a tres objetivos: 1) tipo, nivel y evolución a lo largo del tiempo del compromiso con la ciberseguridad, 2) progreso y seguimiento en el grado compromiso con la ciberseguridad desde una perspectiva global y regional, y 3) la división del compromiso de seguridad cibernética o la diferencia entre países en términos de su nivel de participación en iniciativas de ciberseguridad.

Por último, hay que aclarar que el GCI (2018) evalúa a 194 países y otorga una calificación que va del 0 al 100 por ciento, en la que cien representan el mayor compromiso con la AGCS, y 0 la ausencia total de compromiso.

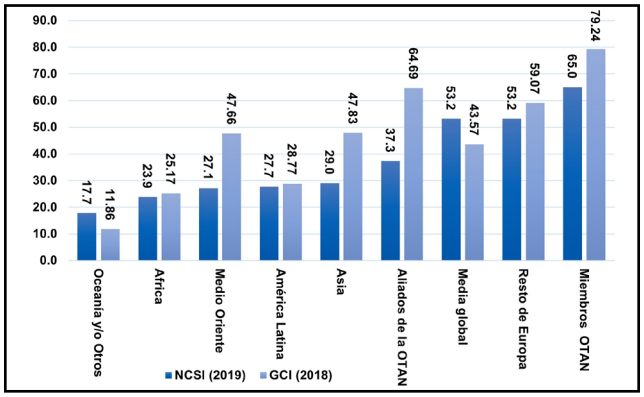
Para ubicar el papel del nivel de ciber capacidades en el que está ubicado América Latina respecto a otras regiones o conjunto de países del mundo, Aguilar-Antonio (2020) agrupó el total de naciones incluidas en el GCI (2018) y el NCSI (2019) en ocho diferentes grupos, que son: 1) Países de la OTAN, 2) Aliados de la OTAN, 3) Resto de Europa, 4) Asía, 5) Medio Oriente, 6) América Latina, 7) África y 8) Oceanía y otros. De cada conjunto se obtuvo el promedio del total de la calificación asignada a cada país que oscila entre 0 y 100, a la que se calculó la media global en cada métrica, los resultados de este análisis se muestran en la Figura 1 con el comparativo entre los dos índices.

En la figura 1 se puede observar que el grupo de países que más ha priorizado el desarrollo de ciber capacidades y mostrado el mayor compromiso con la AGCS son los miembros de la OTAN, de hecho, este conjunto de países se encuentra mejor preparado para atender ciber incidentes o amenazas a la seguridad nacional provenientes del ciber espacio.

Por lo cual, detentan las calificaciones más altas en ambas métricas, con ponderaciones del 79.2 sobre 100, para el NCSI (2019), y 65 puntos para el GCI (2018).

Del mismo modo, destacan grupos como el del resto de Europa con notas de 59.1 y 53.2, respectivamente, y Aliados de la OTAN, que del mismo modo cuentan con los recursos necesarios para enfrentar una crisis proveniente del ciberespacio, con ponderación de 64.9 y 37.3. Con relación a América Latina esta se encuentra en la sexta posición con una calificación de 28.8 para el GCI (2018), y sólo por delante de regiones como África, Oceanía y otros. Para el caso de NCSI (2019) la región se encuentra en la quinta posición con una nota de 27.7, por último, se destaca que en ambas mediciones Latinoamérica se encuentra por debajo de la media global con 25.5 y 14.8 puntos, respectivamente.

Figura 1.
Comparativo regional y global entre ponderaciones del GCI (2018) y el NCSI (2019).



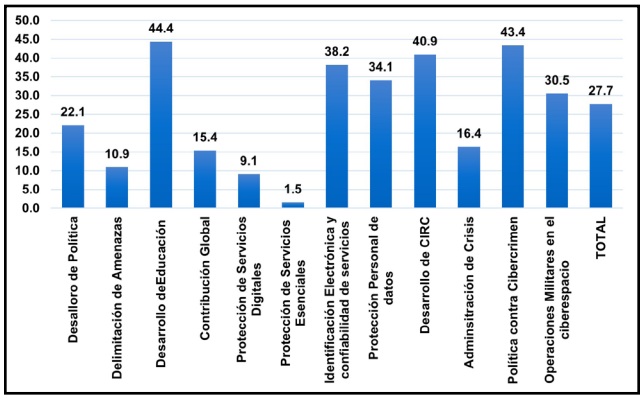
Fuente: Elaboración propia.

Por su parte, los doce indicadores del NCSI (2019) presentan un análisis de trascendencia para comprender las razones que explican los límites y áreas de oportunidad en el desarrollo de capacidades cibernéticas en la región. Para esto podemos observar la figura 2, en la que se destaca que las dos dimensiones entre las que mejor se encuentra posicionada la región son el desarrollo de política contra ciber crimen (43.4) y desarrollo de educación (44.4).

Sin embargo, la región no ha logrado una definición concisa de qué tipos de ciber amenazas pueden afectar su seguridad nacional (10.9 puntos sobre un total de cien), a la par que su desarrollo de ENCS aún tiene un valor bajo (22.1), al mismo tiempo que las capacidades de sus fuerzas armadas están aún en desarrollo para enfrentar ciber amenazas (30.5).

Figura 2.

Media de indicadores de capacidades cibernéticas en América Latina.

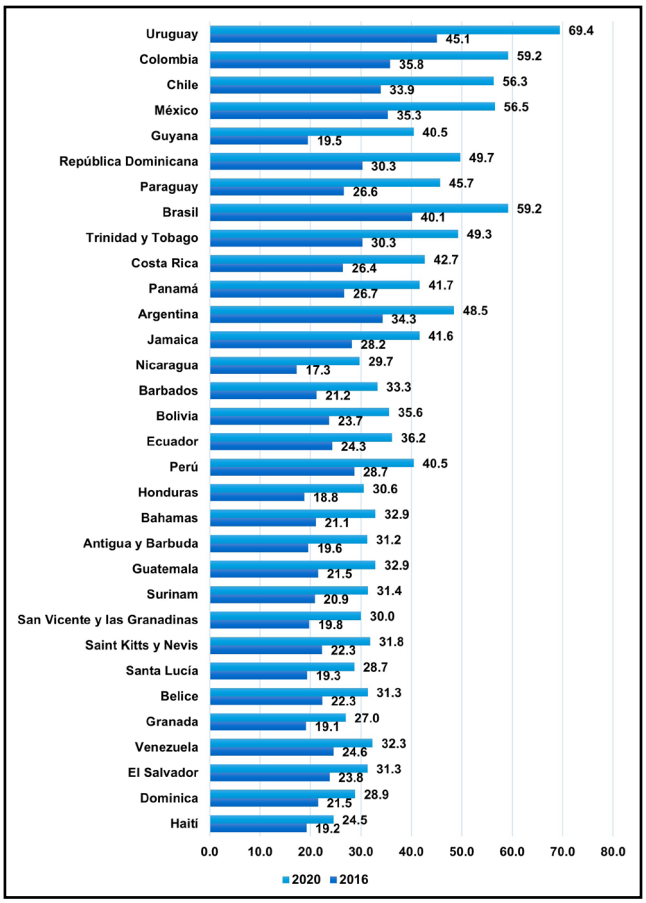


Fuente: Elaboración propia con base a NCSI (2019).

Respecto al seguimiento en materia de ciberseguridad que han dado OEA y el BID se encuentran los informes Ciberseguridad: ¿Estamos preparados en América Latina y el Caribe?, publicado en 2016, y el reporte Ciberseguridad 2020: riesgos, avances y el camino a seguir en América Latina y el Caribe (OEA/BID, 2016;2020). Estos dos documentos permiten evaluar el grado de desarrollo de las ciber capacidades de los países de la región a través de cinco dimensiones y 49 indicadores. La información sobre el progreso de los países en la región se presenta en la figura 3.

Figura 3.

Avance de capacidades cibernéticas de América Latina (2016-2020).



Fuente: Elaboración propia con base a la OEA/BID (2016:2020).

De las dimensiones expuestas, se expresa que las dimensiones de política y estrategia de seguridad cibernética y marcos legales y regulatorios, están vinculadas aspectos de ciber poder y seguridad nacional. Si bien en la figura 3, se presentaron las ponderaciones y avances que alcanzaron los 32 países de América Latina en el periodo 2016-2020.

Revista Académica Seguridad y Estrategia Año 2022. Volumen 1. Número 2. ISSN: 2790-1475

Es importante expresar que los cinco países que más han mejorado en ese lapso fueron Uruguay (con un cambio de 24.4), Colombia (23.4), Chile (22.4), México (21.2) y Guyana (20.9) del mismo modo, los que tuvieron el desempeño más precario en la elaboración de una política de ciberseguridad fueron Granada (7.9), Venezuela (7.8), El Salvador (7.5), República Dominicana (7.4) y Haití (5.4).
Es importante destacar que la ponderación nuevamente va del 0 al 100 y este nivel de mejoría se puede observar en la tabla 1.

Tabla 1.
Puntos de mejora en la ponderación de los informes del BID/OEA (2016;2020)

No.	País	Δ Cambio 2016-2020	No.	País	Δ Cambio 2016-2020
1	Uruguay	24.4	17	Ecuador	11.8
2	Colombia	23.4	18	Perú	11.8
3	Chile	22.4	19	Honduras	11.8
4	México	21.2	20	Bahamas	11.8
5	Guyana	20.9	21	Antigua y Barbuda	11.7
6	República Dominicana	19.4	22	Guatemala	11.4
7	Paraguay	19.1	23	Surinam	10.5
8	Brasil	19.0	24	San Vicente y las Granadinas	10.3
9	Trinidad y Tobago	19.0	25	Saint Kitts y Nevis	9.5
10	Costa Rica	16.3	26	Santa Lucía	9.4
11	Panamá	15.0	27	Belice	9.0
12	Argentina	14.2	28	Granada	7.9
13	Jamaica	13.4	29	Venezuela	7.8
14	Nicaragua	12.5	30	El Salvador	7.5
15	Barbados	12.1	31	Dominica	7.4
16	Bolivia	11.9	32	Haití	5.4

Fuente elaboración propia con base OEA/BID (2016;2020).

Respecto a las dimensiones de Política y Estrategia de Seguridad Cibernética y Marcos Legales y Regulatorios, se destaca el liderazgo de Uruguay, Colombia y Chile, quienes han manejado un política consistente y continua de proyecto como el Fortalecimiento de la Ciberseguridad en Uruguay, la aprobación de la segunda ENCS de Colombia y la promulgación de la Ley Marco de Ciberseguridad en Chile, así como la mejora y establecimiento del Sistema Nacional de Ciberseguridad, de dicho país.

En menor medida, destacan lo realizado por México con la creación de su primer ENCS, en 2017, y la presentación de cinco propuestas legislativas vinculadas a ciberseguridad en el gobierno de México durante el periodo 2018-2021. Y por Guyana que en 2018 promulgó una legislación sobre delitos cibernéticos, así también en 2019 creó un Grupo de Trabajo de Estrategia Nacional de Ciberseguridad.

Análisis prospectivo de América Latina para 2030

La aplicación de métodos prospectivos de carácter cualitativo al entorno de desarrollo de capacidades cibernéticas de América Latina y los escenarios de futuros, implica plantear tres interrogantes:

¿Qué problemas plantea para la seguridad nacional el desarrollo deficiente o nulo de una ENCS efectiva?

¿Qué afectaciones tendrían los países de América Latina al quedarse rezagados frente al vertiginoso avance de las nuevas tecnologías como la computación cuántica y las redes 5G?

¿Qué capacidades de reacción tendría la región frente a un severo caso de ciber incidente o ciber ataque a infraestructura nacional critica, fuga de información o ciber explotación en 2030?

Frente a estos cuestionamientos de cara al futuro, los instrumentos del GCI (2018), NCSI (2019), y los informes de la OEA/BID (2016;2020) fungen como elementos para realizar un diagnóstico estratégico en el marco de nuestro ejercicio prospectivo que sirve para identificar y analizar las tendencias o variables internas y el entorno en el que se circunscribe está problemática para la seguridad nacional.

En ese sentido, se destaca que con base a dichas métricas y reportes internacionales, se procedió a su conceptualización y análisis mediante identificación de variables en las que las naciones están mejor posicionadas o han alcanzado los mejores resultados, y aquellas en las que se presenta el desempeño más precario.

Lo anterior, a razón de que se considera que estas representan las variables portadoras de futuro que se caracterizan por su dinamismo para analizar la influencia y dependencia a través del análisis estructural. De esta forma, se recurrió a una matriz de análisis estructural de variables para su conversión a factores con potencial de influir en los futuros, para identificar las fortalezas, debilidades, amenazas y oportunidades de la región, que se presenta en la tabla 2.

Tabla 2.

Matriz de análisis tendencial de desarrollo de ciber capacidades de América Latina.

Análisis Estructural	Variables	Indicadores
Fortalezas	Interés y voluntad gubernamental en el desarrollo de política contra cibercrimen.	Política de cibercrimen
	Avances significativos en el desarrollo de Centros de Cómputo de respuesta ante incidentes informáticos (CIRC).	Desarrollo de CIRC
	Avances significativos en el desarrollo de programas académicos y educativos para formar especialistas en ciberseguridad.	Formación de capital humano en ciberseguridad
Debilidades	Nulo desarrollo en acciones y política de protección de servicios esenciales en materia de ciberseguridad.	Protección de servicios esenciales
	Nulo desarrollo en acciones y política de protección de servicios digitales.	Protección de servicios digitales
	Precario y lento avance en estructuración de una ENCS y delimitación de ciber amenazas al Estado-Nación.	Desarrollo de ENCS
Oportunidades	Priorizar el tema de ciberseguridad como elemento trascendental de la seguridad nacional.	Promover acciones para desarrollo ENCS
	Promoción de alianzas estratégicas entre partes interesadas para promover capacidades de ciberseguridad en México).	Vinculación de partes interesadas
	Formación de especialistas en ciberseguridad con un enfoque técnico, legislativo-jurídico y estratégico.	Fomento a la formación capital humano
Amenazas	Potencial de no contar con el capital humano en materia de ciberseguridad en 2030 y tener que contratar servicios a empresas o actores extranjeros con alto costo para el gobierno y empresas privadas.	Carencia de capital humano estratégico
	Rezago y brecha para obtener beneficios del ciberespacio respecto a naciones líderes en ciberseguridad y tecnologías de IA, Computación Cuántica, Redes 5G, etc.	Rezago internacional frente beneficios del ciberespacio
	Fracaso en la consolidación de una ENCS y agencias nacionales de ciberseguridad que coordinen de forma efectiva una política de ciberseguridad que abone al poder nacional.	Fracaso de consolidación de ciber poder y ENCS
	Alto potencial de ciber agresores para vulnerar al Estado-Nación, empresas privadas y ciudadanía por ausencia de delimitación de amenazas del ciberespacio.	Alta vulnerabilidad frente ciber amenazas

Fuente Elaboración propia con base al NCSI (2018), GCI (2019) y OEA/BID (2016:2020)

Con relación a la figura anterior, se destaca que la delimitación de las variables portadoras de futuro corresponde a los resultados obtenidos del desarrollo de ciber capacidades de América Latina en el análisis de la sección anterior del NCSI (2018), GCI (2019) y OEA/BID (2016:2020). Por ejemplo, para identificar a las variables presentadas como fortalezas y oportunidades, se seleccionó a los indicadores del NCSI (2018) en los que sale mejor evaluada la región de América Latina, en este caso concreto: i) política contra ciber criminen (43.3% de 100%), ii) desarrollo de CIRC (40.9%), iii) desarrollo de educación (44.4%). A la par que los informes de OEA/BID (2016;2020) los que presentaron que las áreas en las que más avanzó la región durante el periodo 2016-2020 fueron i) cultura cibernética y sociedad (con una mejora de 15.97 puntos de un total de cien) y marcos legales y regulatorios (con mejora de 27.81 puntos).

Del mismo modo, para identificar las variables portadoras de futuro incluidas en el análisis estructural como debilidades y amenazas se presentan a las dimensiones en que sale menos aventajada la región respecto a la OEA/BID (2016;2020), en este caso: i) estándares, organizaciones y tecnologías (mejora de 11.49 puntos), formación, ii) capacitación y habilidades de seguridad cibernética (mejora 4.64) y iii) política y estrategia de seguridad cibernética (8.63 puntos de mejora). Del mismo modo, se incluyen los indicadores del NCSI (2018) en los que América Latina presenta el desempeño más precario y preocupante, a saber: i) Protección de servicios esenciales (1.5% de un total de 100%), ii) protección de servicios digitales (9.1% de un total de 100%), y iii) delimitación de amenazas (10.9% de un total de 100%) y desarrollo de ENCS (22.1 %).

A partir de la matriz de análisis estructural se realiza el método de análisis morfológico de Fritz Zwicky, que se fundamenta en la construcción de escenarios futuros correlacionados a los factores estratégicos y variables portadoras de futuro (Valero y Rodríguez,2019; Mancipe y Pardo, 2017). En este caso se tiene en cuenta un escenario positivo y un escenario negativo con base a cada variable portadora de futuro para el 2030. La información se presenta en la tabla 3.

Tabla 3.

Matriz de escenarios morfológico

No.	Variable	Escenario Positivo 2030	Escenario Negativo 2030
1	**Política de cibercrimen**	América Latina tiene una política efectiva de cibercrimen capaz de sancionar al 80% de actores que ejecutan una actividad ilícita frente al cibercrimen.	80% de los países de América Latina no cuenta con legislaciones o un marco jurídico para combatir el cibercrimen.
2	**Desarrollo de CIRC**	Los CIRC de los países de América Latina tienen un nivel de ciber resiliencia de 80% frente a incidentes de ciberseguridad.	Los CIRC de América Latina tienen un rezago y constantemente se ven superados por agresiones del ciberespacio.
3	**Formación de capital humano en ciberseguridad**	Los países de América Latina pueden cubrir 85% de la demanda de especialistas en ciberseguridad a través de programas de formación y capital humano nacional, del mismo modo se hacen aportes de conocimiento global.	América Latina tiene una sobre demanda de especialistas en ciberseguridad. Los programas de formación y capital humano nacionales sólo cubren 15% y el resto de mercado corresponde a especialistas extranjeros de alto costo.
4	**Desarrollo de ENCS**	Los países de América Latina tienen una ENCS de carácter dinámico, van en la 3 o 4 versión del documento y se actualizan respecto a tendencias globales.	40% de los países de la región siguen sin una primera versión de su ENCS. Los países que cuentan con una no la han actualizado a tendencias globales y es un documento alejado de la realidad
5	**Delimitación de ciber amenazas**	América Latina tiene bien delimitadas sus amenazas y vulnerabilidades desde la arena del ciberespacio, así como los riesgos que pueden acontecer para afectar al Estado-Nación.	Los gobiernos de los países no conocen el potencial de las ciber amenazas, constantemente hay ciber ataques con altas pérdidas a la seguridad nacional del Estado-Nación.
6	**Protección de servicios esenciales y digitales**	Existen las medidas suficientes de ciber resiliencia para garantizar la continuidad de servicios esenciales y digitales para el 85% de las amenazas provenientes del ciberespacio.	Los ciberataques pueden afectar e interrumpir completamente el funcionamiento de servicios esenciales y digitales. El gobierno e instituciones privadas tarden semanas, a veces meses, en resolver un ciber incidente.
7	**Vinculación de partes interesadas**	Existe una agencia o entidad coordinadora en materia de ciberseguridad que ha delimitado responsabilidad y obligaciones de las partes interesadas en materia de ciberseguridad.	Existen esfuerzos descoordinados y sin ningún impacto para crear capacidades de ciberseguridad. El gobierno, instituciones privadas y población avanzan hacia vías divergentes y no conciliadoras.
8	**Brecha tecnológica para obtener beneficios del ciberespacio**	América Latina se encuentra con un ligero rezago frente a tendencias globales de tecnologías 5G, IA, computación cuántica y Big Data. No es capaz de explotar al 100% estás tecnologías, pero obtiene beneficios económicos y para la seguridad nacional de los mismos.	América Latina como región está completamente rezagada frente a tendencias globales de tecnologías 5G, IA, computación cuántica y Big Data. Es imposible acceder a los beneficios económicos y para la seguridad nacional de los mismos.

Fuente: Elaboración propia.

La matriz de escenarios de análisis morfológico anterior, sirve de punto de partida de recomendaciones y consideraciones que los países deben tener en el futuro cercano para la consolidación de política y estrategia nacional de ciberseguridad de cara al 2030. Con poder potencializar las oportunidades y fortalezas que detenta en la actualidad, así como disminuir sus debilidades y amenazas en el ciberespacio en el futuro cercano.

Conclusiones

En la actualidad el ciberespacio se ha transformado en una nueva arena de interacción, cooperación y conflicto para la seguridad nacional. En ese sentido, destaca cómo en la última década las amenazas y riesgos provenientes de ciberespacio se han incrementado. Transformando a la ciberseguridad en un tema central para alcanzar el futuro deseado de los Estados-Nación. Los rápidos avances en tecnología han hecho del ciberespacio un dominio trascendental para garantizar la seguridad nacional del Estado-Nación, y un elemento clave del análisis prospectivo para garantizar el futuro deseado de un país.

En el ámbito global de la ciberseguridad, destaca el papel de organismos como la ITU al crear la AGCS que marca una línea de acciones de los países del mundo para desarrollar una política de ciberseguridad y crear capacidades cibernéticas para enfrentar los riesgos provenientes del ciberespacio. A razón de la AGCS se han estructurado importantes métricas como el GCI (2018) y el NCSI (2020) que permiten ver el avance de los países en el nivel individual y grupal, y permiten ver la brecha regional que detenta Latinoamérica en la construcción de ciber capacidades respecto a otro conjunto de naciones y regiones del mundo, como los países integrantes de la OTAN, Europa o Asía.

También, es importante destacar el liderazgo de la OEA/BID (2016;2020) con la publicación en el ámbito latinoamericano, que para el periodo 2016-2020, permiten analizar el grado de avance de los países y mejoría en el desarrollo de su política

Para el caso concreto de los escenarios futuros obtenidos a través de la matriz de análisis tendencial se idéntico a variables portadoras de futuro a aspectos como : i) Política de ciber crimen, ii) Desarrollo de CIRC, iii) Formación de capital humano en ciberseguridad, iv) Desarrollo de ENCS, v) Delimitación de ciber amenazas, vi) Protección de servicios esenciales y digitales, vii) Vinculación de partes interesadas, viii) Brecha tecnológica para obtener beneficios del ciberespacio.

A partir de estas variables se enmarcan una serie de acciones para mejorar las capacidades cibernéticas de América Latina frente al contexto global de 2030 y resolver tres importantes problemas vinculados a la ciberseguridad que son: el desarrollo de ENCS, rápido avance de tecnologías del ciberespacio y capacidades de acción del Estado-Nación ante amenazas del ciberespacio para América Latina en el 2030.

Referencias Bibliográficas

Aguilar-Antonio, J.-M. (2019). Hechos ciberfísicos: una propuesta de análisis para ciberamenazas en las Estrategias Nacionales de Ciberseguridad. URVIO. Revista Latinoamericana De Estudios De Seguridad, (25), pp. 24-40.

Choucri, N., Madrick, S. Ferwerda, J. (2013). Institutional Foundations for Cyber Security: Current Responses and New Challenges. MIT. Massachusetts, EUA, 27 pág.

Cybersecurity Ventures. Cybercrime To Cost The World $10.5 Trillion Annually By 2025. Recuperado el 12 de enero de 2020 de: https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

Digital Attack Map (2021). Digital Attack Map. Recuperado el 12 de enero de 2021de: https://www.digitalattackmap.com/

GCI (2018). Global Cybersecurity Index. International Telecommunication Union, Recuperado el 12 de enero de 2021 de: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

Gray, C. & Sloan, G. (1999). Geopolitics, Geography and Strategy, Routledge Taylor & Francis Group, Oxfordshire: United Kingdom, 298 pág.

Hackmageddon. 2020 Cyber Attacks Statistics. Recuperado el 12 de enero de 2020: https://www.hackmageddon.com/category/security/cyber-attacks-statistics/

Kapersky. Kaspersky Lab registra un alza de 60% en ataques cibernéticos en América Latina. Recuperado el 12 de enero de 2020: https://latam.kaspersky.com/blog/empresas-principal-objetivo-de-ciberataques-en-america-latina/20209/

Kuehl, D. T. (2009). From Cyberspace to Cyberpower: Defining the Problem", en Franklin D. Kramer, Stuart H. Starr, Larry K. Wentz. Cyberpower and National Security, Washington D.C.: National Defense University Press, pp. 25-42.

Mancipe, F. y Pardo, I. (2017). Estudio Prospectivo de la Organización Acceso Colombia ESAL al año 2026. Universidad Externado de Colombia, Bogotá, D.C., Colombia NCSI (2019). National Cyber Security Index. E-Governance Academy, Recuperado el 12 de enero de 2021 de: https://ega.ee/wp-content/uploads/2018/05/ncsi_digital_smaller.pdf

Nye, J. (2010). Cyber power. Harvard Univ Cambridge MA Belfer Center for Science and International Affairs.

Nye, J. (2014). The regime complex for managing global cyber activities. Belfer Center for Science and International Affairs, John F. Kennedy School of Government, Harvard University, 32 pág.

OEA & (BID) Banco Interamericano de Desarrollo. (2016). Ciberseguridad: ¿Estamos preparados en América Latina y el Caribe? 193 pág. Recuperado el 12 enero de 2021 de: https://publications.iadb.org/es/publicacion/17071/ciberseguridad-estamos-preparados-en-america-latina-y-el-caribe

OEA & BID (2020). Reporte Ciberseguridad 2020: riesgos, avances y el camino a seguir en América Latina y el Caribe. 204 pag. Recuperado el 12 enero de 2021 de: https://publications.iadb.org/es/reporte-ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-america-latina-y-el-caribe

Peláez, M., Álvarez, Y., Palacio, I. y Mazo, A.(2017). Aplicación de los ejes de Schwartz como metodología de prospectiva tecnológica al modelo universitario-empresa en el contexto colombiano. Revista Ingenierías USBMed, 8(1), 63–70.

Sheldon, J. (2012). "Deciphering Cyberpower: Strategic Purpose in Peace and War." Strategic Studies Quarterly, vol. 5, no. 2, 2011, pp. 95–112.

Sicherheitstacho. Overview of Current Cyber Attacks. Deutsche Telekom. Recuperado el 12 de enero de 2021 de: https://www.sicherheitstacho.eu/start/main

Starr, S. H. (2009). Toward a preliminary theory of cyberpower. en Franklin D. Kramer, Stuart H. Starr, Larry K. Wentz. Cyberpower and National Security, Washington D.C.: National Defense University Press, pp. 43-88.

Valero, L. & Rodríguez, R. (2019). Estudio prospectivo de escenarios de la tecnología en el trabajo en Colombia al 2050. ECONÓMICAS CUC, 40(2), 101-116.

Juan Manuel Aguilar Antonio

Doctor en Ciencias Sociales por la Facultad de Ciencias Políticas y Sociales, de la Universidad Nacional Autónoma de México (UNAM). Egresado del curso Desarrollo de Políticas Cibernéticas del Centro William J. Perry (2019). E Investigador Senior del Colectivo de Análisis de Seguridad con Democracia (CASEDE AC) en México.

Los errores remanentes son responsabilidad de los autores.

Revista Académica Seguridad y Estrategia Año 2022. Volumen 1. Número 2. ISSN: 2790-1475