"ENFRENTANDO LAS CIBERAMENAZAS: ESTRATEGIAS NACIONALES DE CIBERSEGURIDAD EN EL CONO SUR"

Facing Cyber Threats: National Cybersecurity Strategies in the Southern Cone

Recibido: 09 / 09 / 2019 Aprobado: 30 / 10 / 2019

Doctora
Lucia Dammert
Chile

Doctora en Ciencia Política en la Universidad de Leiden, Holanda. Socióloga. Ha trabajado en instituciones académicas en Estados Unidos, Argentina, y Chile. En la actualidad es Profesor Asociado de la Carrera de Estudios Internacionales de la Facultad de Humanidades de la Universidad de Santiago de Chile. Ha publicado artículos y libros sobre participación comunitaria, seguridad ciudadana, conflictividad social y temas urbanos en revistas nacionales e internacionales. En el plano de la gestión pública ha participado de programas de seguridad ciudadana en diversos países de la Región. Ha realizado asesoría a diversos gobiernos entre los que destacan Chile, Argentina, Perú y México. Se desempeñó además como asesor experto en el Departamento de Seguridad Públlica de la Organización de los Estados Americanos y como Consultor Banco Interamericano del Desarrollo, Banco Mundial, Programa de Naciones Unidas para el Desarrollo, CAF, entre otros organismos regionales y multilaterales. Miembro de la Junta Directiva de UNIDIR (United Nations Institute for Disarmament Research), del Directorio del Centro de Pensamiento Espacio Público, de Asuntos del Sur y de la Fundación Junto al Barrio. Es parte del Consejo Asesor en Temas de Desarme del Secretario General de Naciones Unidas para el periodo 2017-2020 siendo la única representante de América Latina. lucia.dammert@usach.cl

Licenciada
Constanza Núñez
Chile

Licenciada en Estudios Internacionales por la Universidad de Santiago de Chile y Analista en Política y Asuntos Internacionales de la misma casa de Estudios. Actualmente trabaja temas de ciberseguridad. constanza.nunez.c@usach.cl

RESUMEN

En los últimos años, las amenazas cibernéticas han aumentado entre 30% y 40% en América Latina, posicionándose como la región en la que con mayor rapidez se presentaron este tipo de ataques. En este contexto hostil el presente artículo analiza las Estrategias Nacionales de Ciberseguridad desarrolladas por los países del Cono Sur tomando como referencia los lineamientos desarrollados por la OECD para este tipo de situaciones. Los avances son innegables, pero se concentran aún en las tareas procedimentales y discursivas, en general los países analizados se encuentran bastante desprovistos de mecanismos efectivos para enfrentar las ciberamenazas y su potencial desarrollo en el corto plazo.

Palabras clave:
Cono Sur, ciberseguridad, OECD, políticas públicas.

ABSTRACT

In recent years, cyber threats have increased between 30% and 40% in Latin America, positioning itself as the region in which this type of attack occurred most rapidly. In this hostile context, this article analyzes the National Cybersecurity Strategies developed by the Southern Cone countries, taking as a reference the guidelines developed by the OECD for this type of situation. Progress is undeniable, but they are still focused on procedural and discursive tasks, in general the countries analyzed are quite devoid of effective mechanisms to deal with cyber threats and their potential development in the short term.

Keywords:
Southern Cone, cibersecurity, OCDE, public policies.

INTRODUCCIÓN

La diversificación de los usuarios de internet ha provocado que, en los últimos años aumenten con rapidez las interconexiones globales basadas en transmisiones de alta velocidad, estableciendo relaciones cibernéticas casi instantáneas provenientes de distintos puntos del planeta, robusteciendo el mundo virtual más conocido como ciberespacio. América Latina no está fuera de este proceso, de hecho es una de las regiones donde "la población de usuarios de internet ha crecido más rápido en el mundo (OEA & Symantec; 2014: p.11). Este importante acceso a internet trae consigo múltiples factores positivos para el desarrollo de las personas, países e instituciones, tales como: Gobierno electrónico, comercio electrónico, comunicación e información instantánea, banca en línea, diversos servicios públicos y privados ejecutables vía web. Sin embargo, también genera un ambiente idóneo para la producción y desarrollo de delitos cibernéticos, puesto que las características intrínsecas de internet tales como el anonimato y la capacidad de actuar a distancia con costos limitados, permiten vulnerar el normal funcionamiento de los usuarios conectados a la red.

En América Latina y el Caribe, a nivel general, "se produjeron 253 violaciones de datos a gran escala en el 2013, lo que representó un aumento del 62% respecto del año 2012." (OEA & Symantec; 2014, p.11). Esta situación empeora cuando ponemos el foco en la sociedad civil, puesto que "ocho de estas violaciones de datos expusieron 10 millones de identidades o más cada una, lo cual obligó a comerciantes minoristas, empresas financieras y de seguros, y personas físicas a invertir una gran cantidad de tiempo y recursos financieros para responder y recuperarse de esos ataques e implementar mecanismos de protección adicionales." (OEA & Symantec; 2014, p.11). En efecto, la situación expuesta nos muestra el déficit de seguridad que hay en el ciberespacio.

La amenaza es global y requiere de respuestas de igual magnitud. Organizaciones Internacionales tales como: Organización de las Naciones Unidas[1], Organización Tratado Atlántico Norte[2], Unión Europea[3], Organización de Cooperación de Shanghái[4], Organización para la Cooperación y el Desarrollo Económico[5], Organización de Estados Americanos[6], Liga de los Estados Árabes[7] y Unión Africana[8], proponen lineamientos, estrategias y objetivos a sus respectivos países miembros con la finalidad que la seguridad cibernética cumpla estándares internacionales básicos como también elaborar un ambiente regional seguro en materia informática. Especialmente el marco propuesto por la OECD permite enfrentar las ciberamenazas desde distintos niveles de impacto así como desde múltiples perspectivas institucionales por lo que lo consideramos un marco de referencia apropiado para realizar un análisis comparado de iniciativas nacionales.

En consecuencia, en América Latina, diversos gobiernos han comenzado a elaborar o actualizar sus respectivas Estrategias Nacionales de Ciberseguridad (desde ahora, ENCS) con el objetivo de modernizar los resguardos nacionales en asuntos cibernéticos y hacer frente a las amenazas emergentes provistas por las nuevas tecnologías. De hecho, se torna vital asegurar el ciberespacio ya que es "una cuestión nacional estratégica que afecta a todos los niveles de la sociedad" (Leiva, 2015, p.163), mermando no solo el normal funcionamiento gubernamental y privado en el caso que no se tomen las medidas suficientes y a tiempo, sino que también deteriorando las relaciones entre los diversos actores que se desenvuelven en la esfera nacional e internacional. En este mismo sentido, es imprescindible el desarrollo de investigaciones que permitan comprender la nueva configuración de amenazas presentes en los temas de seguridad nacional e internacional. (Organización para la Cooperación y el Desarrollo Económico, 2012).

El presente artículo analiza las ENCS de cinco países del Cono Sur, Argentina, Brasil, Chile, Paraguay y Uruguay, a partir del marco analítico propuesto por la OECD como parámetro de comparación. El objetivo es conocer la preparación de la ciberseguridad de cada Estado mostrando diferencias y similitudes entre sus respectivas estrategias, entendiendo que los riesgos tradicionales, cada vez pierden relevancia, posicionándose otros que tienen una importante dimensión virtual sumado al constante desarrollo, por tanto, es imperativo que los Estados tomen medidas y desarrollen políticas robustas en materia de ciberseguridad (Núñez, 2019).

[1] https://www.un.org/es/
[2] https://www.nato.int/
[3] https://europa.eu/european-union/index_es
[4] http://eng.sectsco.org/
[5] http://www.oecd.org/
[6] http://www.oas.org/es/
[7] http://www.lasportal.org/ar/Pages/default.aspx
[8] https://au.int/

CIBERESPACIO, CIBERAMENAZAS Y CIBERSEGURIDAD

Desde fines del siglo XX, hemos visto cómo las nuevas tecnologías y el acceso a internet han modificando nuestras vidas desde lo más cotidiano hasta las formas más complejas de interacciones en las distintas esferas de la sociedad. De cara a la expansión tecnológica, el autor Van Bendegem (2016) reconoce que este fenómeno emergente trae serios cambios a las estructuras sociales, económicas y políticas, incluyendo una reformulación del orden mundial basado en la Paz de Westfalia.

Desde el ámbito de la Defensa Nacional, de igual manera, se reconoce una quinta dimensión. Ruiz (2010) señala, a veces virtual y a veces real, es un nuevo espacio para el desarrollo de la guerra y por ende una nueva dimensión que se debe asegurar. Esta nueva dimensión conocida también como ciberespacio es un ambiente de "grandes oportunidades, pero también es imposible ocultar que, en él, se tensionan los intereses de los Estados con fines distintos, organizaciones terroristas y redes de crimen organizado [los cuales] se sirven de las facilidades que se ofrece el medio." (Moreno y Gil, 2017, p.65) para realizar ciberamenazas.

A partir de los planteamientos de Ruiz, "podríamos definir las ciberamenazas, como aquellas actividades realizadas en el ciberespacio, que tienen por objeto la utilización de la información que circula por el mismo, para la comisión de distintos delitos mediante su utilización, manipulación, control o sustracción" (2016, p.3). En relación con lo anterior, se pueden identificar al menos nueves actores los que pueden generar ciberamenazas, estos son: Estados, ciberdelincuentes, grupos terroristas, grupos yihadistas, cibervándalos, hacktivistas, actores internos, ciberinvestigadores y organizaciones privadas. (Fernández y Rodríguez, 2017). Cada uno de estos agentes, plantean sus objetivos dependiendo del sector que quieran amenazar/atacar y del nivel de peligrosidad que quieran causar. Teniendo en cuenta la diversidad de las ciberamenazas que se pueden realizar por medio del ciberespacio y lo variado que son sus ejecutores, es que se hace necesario contar con medidas de seguridad para esta nueva dimensión por medio de compromisos por parte de las instituciones para cumplir con los requerimientos básicos de ciberseguridad.

Es por ello que, Hirare propone que "la ciberseguridad constituye una condición para permitir que los ciudadanos, las organizaciones e instituciones puedan beneficiarse del uso del ciberespacio como dimensión, en la cual las relaciones sociales puedan efectuarse en forma más rápida y económica en comparación con otras formas conocidas de intercambio de información." (2017, p.8).

De ahí la importancia de que las instituciones trabajen y colaboren para desarrollar de manera robusta herramientas políticas y técnicas que beneficien a la ciberseguridad. A nivel internacional encontramos en esta materia que distintos organismos internacionales han trabajado para fortalecer esta área entregando a los Estados líneas de acción y estrategias concretas. Algunos de estos organismos son: la Organización del Tratado del Atlántico Norte[9], la Unión Europea[10], la Unión Internacional de Telecomunicaciones[11], la Organización para la Cooperación y el Desarrollo Económico[12], la Organización de Estados Americanos[13] y Organizaciones de normalización y gestión de internet tales como: Corporation for Assigned Names and Numbers (ICANN), la Internet Engineering Task Force (IETF), la Internet Governance Forum (IGF) y la Inter-

[9] Su trabajo en área cibernética comenzó en el año 1999 en el marco de la Cumbre de Washington D.C., en la que se aprobaron importantes decisiones sobre la capacidad de defensa como en la seguridad para sistemas de comunicación e información de vulnerabilidades. (Gobierno de España, 2014) Desde la fecha se ha ampliado y fortalecido el trabajo a un ritmo acelerado debido al impacto y dinamismo de las tecnologías.
[10] Su célebre trabajo en ciberseguridad y ciberdefensa se enmarca en la Agenda Digital para Europa el cual tiene por objetivo garantizar el crecimiento inteligente de las instituciones y ciudadanos a nivel comunitario. (Gobierno de España, 2014)
[11] Desde el año 1949 es el organismo especializado en el área de las telecomunicaciones de la ONU. "Ha desempeñado un papel importante en las telecomunicaciones mundiales, en la seguridad de la información y en la definición de las normas en los diferentes dominios de las TIC." (Gobierno de España, 2014: 82)
[12] Su trabajo comienza en la década de los 80, desde ahí que este organismo internacional "ha acumulado una amplia experiencia en el debate y discusión de los diversos aspectos relacionados tanto con la seguridad de los sistemas y redes de información como de otras áreas relacionadas, incluyendo la autenticación electrónica, la política de cifrado y la protección de infraestructuras de información crítica." (Gobierno de España, 2014:83) En el año 2002 publica las Directivas de la Seguridad de las TIC, publicación que hace de esta OI uno de los más eficientes en materia de ciberseguridad.
[13] En 2004, la OEA se convirtió en el primer organismo regional en adoptar una estrategia de Seguridad Cibernética a través de la aprobación unánime de "La Estrategia Integral de Seguridad Cibernética Interamericana", que le establece un mandato a la Secretaría General de la OEA en el sentido de ayudar a los Estados miembros en la creación y el fortalecimiento de sus capacidades de seguridad cibernética." (Organización de Estados Americanos,2015:2)

net Society (ISOC)[14], son algunas reconocidas iniciativas mundiales que, hasta la actualidad, fomentan y colaboran a consolidar su capacidad de reacción y respuesta frente a amenazas a los distintos países del globo, respondiendo contundentemente a la necesidad de los Estados y de la misma Sociedad Internacional por instancias supranacionales en esta materia.

PROBLEMAS CIBER EN EL CONO SUR

Realizar un diagnóstico detallado de los delitos o ataques ciber que han ocurrido es aún una tarea pendiente debido a la carencia de registros sólidos así como a los bajos niveles de denuncia de algunos hechos (Núñez, 2019). Sin embargo, se puede afirmar que la tendencia es creciente, que los ataques se destinan a individuos, empresas e instituciones estatales y que los niveles de impunidad de los mismos son aún muy altos. A continuación se presenta un breve repaso de los principales indicadores que sirven para caracterizar la situación.

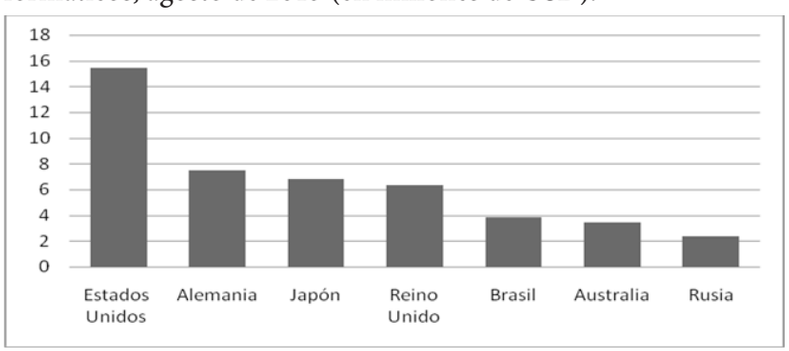
Argentina por años ha sido víctima de distintos tipos de ciberamenazas las cuales han logrado vulnerar las instituciones públicas, privadas y a cientos de ciudadanos. Uno de los más conocidos incidentes fue la modificación del discurso presidencia de Néstor Kirchner en marzo de 2005 publicado en el sitio oficial de la Presidencia de la Nación, el cual fue alterado con frases ofensivas hacia la estructura gubernamental y el sistema político. El mencionado incidente cibernético, es el inicio de una serie de ciberamenazas a los sistemas de administración pública que años más tarde se perpetrarían, viéndose atacadas instalaciones tales como: Ministerio de Economía, Infraestructura y Servicios Públicos de la provincia de Salta, Ministerio de la Producción de la Provincia de Santa Cruz, Ministerio de Relaciones Exteriores y Culto, Secretaria de Ambiente y Apoyo Sustentable de la Nación, entre otras. (Borghello y Temperini, 2013).

Con los años, las ciberamenazas en la Argentina se diversificaron, ya que los ataques no solo estaban destinados al sector gubernamental, sino también a los privados, como el sector empresarial y bancario, los cuales fueron blancos de la vulneración de sus sistemas de protección.

En el año 2017 Argentina, según datos oficiales del Ministerio de Modernización, sufrió más de tres millones incidentes informáticos siendo principalmente las empresas las protagonistas de las denuncias de ciberataques. Estos números y los afectados, muestran claramente un alza de los riesgos de internet y su vinculación a funciones fundamentales para los Estados. El alza es preocupante, debido a que entre 2016 y 2017, en Argentina los hackeos aumentaron en 700% (Dinatale, 2018).

En Brasil, el 2011 fue el año en el que se puso en jaque la seguridad cibernética del país más grande de América Latina debido a uno de los ciberataques más importantes destinado al sector público, en donde se vulneraron las páginas web oficiales de la Presidencia de la República, del Ejército, varios ministerios, y la empresa petrolera Petrobras. Post ciberataque, el servicio de gobierno que se dedica a la recolección de datos y procesamiento informó que "hubo dos millones de accesos ilegales a las páginas, más de 300.000 se produjeron de manera simultánea, en el mayor ataque de la historia de internet de Brasil." (Arias, 2011). Años más tarde, la situación brasileña parece no mejorar. En 2015, Brasil se situaba en quinto lugar a nivel mundial de los países que más pérdidas percibían por delitos informáticos, acompañando a grandes potencias tales como: Estados Unidos y Alemania, incluso superando a Rusia en pérdidas millonarias (ver gráfico 1).

Gráfico1: Volumen de pérdidas generadas por los delitos informáticos, agosto de 2015 (en millones de USD).



Fuente: Elaboración propia en base a Statista, 2019.

[14] Estas organizaciones, en su mayoría privadas y sin ánimo de lucro, han estado promoviendo y desarrollando un espacio permanente abierto a la reflexión. Sus normas y recomendaciones han sido adoptadas por la comunidad de usuarios de Internet, lo que constituye una herramienta importante en la práctica de la administración y el desarrollo técnico."(Gobierno de España, 2014:85)

Uno de los problemas más persistentes que ha tenido Brasil en cuanto ciberamenazas ha sido el ciberespionaje, así lo revelaron las filtraciones de Edward Snowden, el ex trabajador de la Agencia Nacional de Inteligencia de Estados Unidos (NSA, por sus siglas en inglés) el cual denunció que la NSA espiaba las comunicaciones de personas, gobiernos, empresas, organizaciones internacionales y cualquier usuario que estuviera conectado a la red. Brasil fue uno de los mayores afectado de este proceso debido a que este país "hospeda unos de los cables[15] de fibra óptica más grandes e importantes, aquellos por los que se transfieren los correos electrónicos, tuits o fotos de muchos usuarios de internet en el mundo" (Pardo, 2013).

Sin duda, el ciberespionaje estadounidense a las infraestructuras críticas de la información de Brasil dejó en evidencia las graves falencias en ciberseguridad. Si bien el gobierno brasileño ha reaccionado con cambios normativos dirigidos principalmente a atender estos incidentes y así tratar de evitar episodios similares y proteger información estratégica. El tamaño del mercado que suma más de 140 millones de usuarios conectados a la red, equivalentes al 66% de la población; torna esta tarea en un desafío permanente (Moreno, 2018).

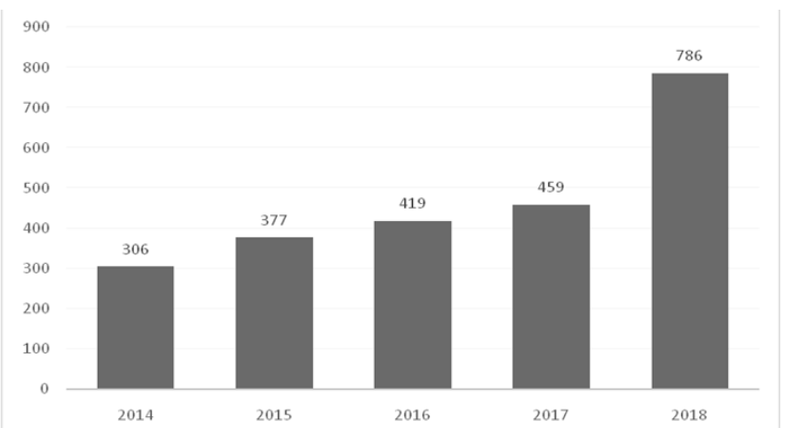
En Chile, desde que el 2000 se incrementó el acceso a internet, ha sido blanco de diversos ciberataques en su mayoría destinados a robar información para cometer fraudes económicos. Si bien estos delitos informáticos en los primeros años eran puntuales, con el paso del tiempo se han convertido en una amenaza más transversal. En el Cyber Monday de 2016, Chile ocupó el quinto lugar en el continente con mayores intentos de ataque repercutiendo en la calidad del servicio (El ciudadano, 2017).

Paraguay, uno de los países más pequeños del mundo, formó parte del listado de los 180 países ciberatacados por el ransomware WannaCry (Frieiro, Pérez y Pascual, 2017) un ataque informático que explota las vulnerabilidades del sistema operativo Windows de Microsoft. El mismo logró encriptar los datos e información crítica de las instituciones gubernamentales, solicitando un pago económico por medio de la criptomoneda Bitcoin para recuperar la información adquirida ilegalmente.

Paraguay, al igual que el resto de los países afectados, maneja sus oficinas públicas con el sistema operativo Windows, por lo que no fue complejo introducir el ransomware de forma transversal (Frieiro, Pérez y Pascual, 2017). El caso paraguayo, si bien no fue tan generalizado como en otros países, igual instaló preocupación e incertidumbre respecto a la capacidad de vulneración de sus sistemas de protección de datos. Uno de los ciberdelitos más reconocidos en este país, es la extorsión sexual hacia menores de edad por medios virtuales. Estos ciberdelitos, que invaden los terrenos más privados de los usuarios de internet, se cometen infectando, a través de un programa informático malicioso, los dispositivos conectados a la red tales como: celulares, Tablet, computadores, notebook, incluso, Smath TV (Segura, 2018).

Uruguay también ha sido víctima de las ciberamenazas. El Centro Nacional de Respuesta a Incidentes de Seguridad Informática de Uruguay (CERTUY) cada año publica las estadísticas de los incidentes registrados desde 2014, con la finalidad de observar la tendencia de amenazas cibernética y poder actuar oportunamente (ver gráfico 2).

Gráfico 2: Número de ciberataques, Uruguay, primer semestre 2014-2018.



Fuente: Elaboración propia en base a los datos de CERTUY.

[15] Los cables submarinos se construyen entre ubicaciones que tienen algo "importante para comunicarse". Europa, Asia y América Latina tienen grandes cantidades de datos para enviar y recibir desde América del Norte. Esto incluye a los operadores de la red troncal de Internet que garantizan que los correos electrónicos y las llamadas telefónicas estén conectados, y los proveedores de contenido que necesitan vincular sus centros de datos masivos entre sí. Esto explica por qué hay tantos cables a lo largo de estas rutas principales. (TeleGeography, 2019)

En el año 2015, hubo un incremento del 23,2% en los incidentes respecto al mismo periodo del año anterior, siendo el Phishing/Spam (36%) y la mala configuración de Hardware/Software (20%) los incidentes más detectados a nivel nacional. (Centro Nacional de Respuesta a Incidentes de Seguridad Informática, 2015). Para 2016 la situación era aún más crítica ya que las instituciones públicas y el sector privado, hasta la fecha, no había recibido tantos ciberataques como ese año. (Natalevich, 2017). En ese mismo año se registraron un total de 768 incidentes a la seguridad informática uruguaya, de los cuales 15 tomaron la categoría de "Alta" mientras que otras seis se manifestaron como incidente de "Muy Alta" categoría. (Centro Nacional de Respuesta a Incidentes de Seguridad Informática, 2016).

Se estima que el crecimiento en la cantidad de ciberataques de Uruguay respondió a múltiples factores de los cuales se destacan: un ambiente generalizado de ciberataques en el mundo, y la implementación de nuevos sistemas y herramientas para la detección de riesgos cibernéticos a nivel nacional.

ESTRATEGIAS NACIONALES DE CIBERSEGURIDAD

Las ENCS buscan responder a las nuevas necesidades de seguridad en el ciberespacio. Si bien hay diversas definiciones, consideramos que son "un plan de acción nacional sobre la base de una visión nacional para lograr un conjunto de objetivos que contribuyan a la seguridad del ciberespacio" [Luiijf et al., 2013]. Se encuentra a un alto nivel en la pirámide organizacional de una nación, y establece una serie de objetivos nacionales y prioridades que deben alcanzarse en un plazo determinado. Como tal, proporciona un marco estratégico para la implementación de un Sistema de Ciberseguridad Nacional, que se entiende como un conjunto de órganos, organismos y procedimientos que permiten la dirección, control y gestión de la Ciberseguridad. (Leiva, 2015, p.163).

Por su parte, la OECD, en su informe Cybersecurity Policy Making at a Turning Point, nos señala que el objetivo de las ENCS es "aumentar la coordinación gubernamental al nivel de políticas y operaciones así como clarificar los roles y responsabilidades de cada institución" (2012, p.9). Ambas definiciones ponen énfasis en el hecho que las ENCS solo incluyen a los órganos pertenecientes a la estructura estatal, sino también definen el rol que cumplen los actores privados y la sociedad civil en esta materia, para que se gestione una efectiva ciberseguridad, en la que la cooperación, la coordinación y los acuerdos son fundamentales.

Después del 2010 los países latinoamericanos han empezado a desarrollar sus políticas para enfrentar este nuevo fenómeno.

En la tabla 1 se describen las ENCS de los países estudiados así como su año de publicación, en la mayoría de casos son de años muy recientes.

Tabla 1: Estrategia Nacional de Ciberseguridad.

País	Nombre de la Estrategia Nacional de Ciberseguridad	Año de publicación
Argentina	Estrategia Nacional de Ciberseguridad	2015
Brasil	Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal	2015
Chile	Política Nacional de Ciberseguridad	2017
Paraguay	Plan Nacional de Ciberseguridad de Paraguay	2017
Uruguay	Agenda Uruguay Digital 2020	2016

Fuente: Elaboración propia, 2019.

Argentina

Argentina se distingue por ser uno de los primeros países de la región en desarrollar un Equipo de Respuesta ante incidentes de seguridad cibernética (CSIRT Argentina). (BID & OEA, 2016). Su funcionamiento comienza a fines de siglo XX, específicamente en 1994, sin embargo, no era mucho el trabajo que en esos años podía realizar debido a que era incipiente la apertura de internet. Para una gestión más eficiente, en 2011 el CSIRT Argentina pasa a ser parte del Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad. (BID & OEA, 2016). Dicho programa vinculado al Ministerio de Defensa, aparte de encargarse de mantener un registro centralizado de las ciberamenazas y de las respuestas de las Fuerzas Armadas frente a estos incidentes, también se encarga de la coordinación de los diversos actores y partes interesadas para la elaboración de una contundente ENCS.

Debido al contexto de ciberamenazas, sumado a la vulnerabilidad de la infraestructura crítica nacional, se pone en un proceso la elaboración de una ENCS más integral, incluyendo otros ministerios y subsecretarías en materia de seguridad cibernética en el

año 2015. Desde entonces, Argentina se ha encargado de elaborar un marco jurídico que proporcione facultad a distintos órganos gubernamentales, con la finalidad de ampliar las respuestas ante las amenazas cibernéticas y romper con la única y tradicional respuesta punitiva frente a estos delitos. Uno de los hechos más importantes que mostró el nuevo camino que la ciberseguridad estaba tomando en el país trasandino fue la creación del Ministerio de Modernización, el cual trabaja con cinco ejes: Modernización Administrativa, Gobierno Abierto, Capital Humano, Infraestructura Tecnológica y Ciudadanía Inteligente. (Ministerio de Modernización, 2019). Este ministerio, en definitiva, llega a enriquecer la oferta ministerial y gubernamental en materia de ciberseguridad. Así desde 2017 el Gobierno argentino trabaja con representantes de los Ministerios de Modernización, Defensa y Seguridad, y Ministerio Público Fiscal conformando el Comité de Seguridad con mira a generar una cultura de ciberseguridad.

Brasil

En el año 2015, en el mandado de la ex Presidenta Dilma Rousseff (2011- 2016), se publica la Estrategia Nacional de Seguridad de las Comunicaciones de Información y Seguridad Cibernética de la Administración Pública Federal 2015 – 2018, la que tiene como misión "fortalecer a política e o planejamento de segurança da informação ecomunicações e de segurança cibernética na Administração Pública Federal, visandoassegurar e defender os interesses do Estado e da sociedade para a preservação dasoberania nacional."[16](Departamento de Segurança da Informação e Comunicações. [DSIC], 2015, p.37)

Para cumplir con lo anterior, la Estrategia de Ciberseguridad de Brasil plantea principios norteadores los cuales ayudarán a direccionar las acciones a nivel nacional respecto a la ciberseguridad. Se plantea un órgano central y un sistema nacional (DSIC, 2015) que realice coordinación, seguimiento y evaluación de la implementación futura de la Política Nacional de SIC y SegCiber. Para ello, la estrategia considera indispensable establecer la definición de gobernanza (DSIC, 2015) en los sistemas de seguridad cibernética para aunar a los múltiples actores y de esa forma, contribuir con la formulación de la Política Nacional de Seguridad de la Información y Comunicaciones de Seguridad Cibernética.

De igual modo, la ENCS de Brasil plantea desarrollar la capacidad de posicionamiento y de respuesta de la nación (DSIC, 2015), entendiendo que existen amenazas cibernéticas que constantemente evoluciona. De ahí que, es necesario la articulación y alianzas entre los sectores públicos y privados, y la cooperación nacional e internacional, para el fortalecimiento de los temas cibernéticos.

La estrategia hace hincapié en las delimitaciones de la Soberanía Nacional (DSIC, 2015), garantizando recursos continuos y adecuados para la protección de Brasil y sus infraestructuras críticas. Finalmente, se plantea la importancia de resiliencia (DSIC, 2015), la cual busca la superación de incidentes cibernéticos, contribuyendo con el aumento de la capacidad de las infraestructuras destinadas a la ciberseguridad.

Chile

En el segundo periodo de la presidenta Michelle Bachelet (2014-2018), se planteó la necesidad de contar con una Política Nacional de Ciberseguridad (PNCS) la cual entregara protección a los usuarios privados y públicos contra posibles incidentes cibernéticos que vulneren la protección de la privacidad de los ciudadanos. (Bachelet, 2014). Para responder a tal necesidad, en el 2015 fue creado el Comité Interministerial sobre Ciberseguridad el cual dentro de sus funciones, debía asesorar al Presidente de la República en materia de seguridad cibernética, proponer una política nacional de ciberseguridad identificando amenazas del ciberespacio tanto global, regional como nacional, encargarse de la coordinación de acciones y planes de los distintos actores y partes interesadas, como también analizar la legislación vigente, proponiendo modificaciones constitucionales, legales y reglamentarias necesarias. (Viollier, 2017).

En el año 2017, la PNCS llega para resguardar la seguridad de las personas en el ciberespacio por medio de garantizar un nivel de seguridad el cual permita el normal desarrollo de las actividades. La idea, es proteger la seguridad del país como de sus habitantes, resguardando las redes y los sistemas informáticos del sector público y privado. También busca la colaboración, coordinación entre las instituciones gubernamentales, organizaciones y entidades privadas, como también la cooperación con otros países y orga-

[16] Traducción propia: Fortalecer la política y la planificación de seguridad de la información y comunicaciones y de seguridad cibernética en la Administración Pública Federal, con el objetivo de asegurar y defender los intereses del Estado y de la sociedad para la preservación de la soberanía nacional.

nismos internacionales, para que el análisis y gestión de las ciberamenazas sea más rápida, generando capacidades de prevención, respuesta y recuperación ante incidentes cibernéticos.

Es por lo anterior, que los objetivos de la PNCS se dividen en dos, uno de corto plazo para ser concretado en los años 2017-2018, y otro de largo plazo el cual se extiende hasta 2022. En relación con el primero, identificado como Agenda de Medidas 2017-2018, se elabora a partir de 41 medidas las cuales especifican políticas públicas a implementar y el órgano responsable de llevarlo a cabo. El segundo consta de cinco objetivos: (i) El país contará con una infraestructura de la información robusta y resiliente, preparada para resistir y recuperarse de incidentes de ciberseguridad, bajo una óptica de gestión de riesgos; (ii) El Estado velará por los derechos de las personas en el ciberespacio, (iii) Chile desarrollará una cultura de la ciberseguridad en torno a la educación, buenas prácticas y responsabilidad en el manejo de tecnología digitales; (iv) El país establecerá relaciones de cooperación en ciberseguridad con otros actores y participará activamente en fotos y discusiones internacionales; y (v) El país promoverá el desarrollo de una industria de la ciberseguridad, que sirva a sus objetivos estratégicos." (Comité Interministerial Sobre Ciberseguridad, 2017).

Paraguay

Bajo la responsabilidad de la Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs) en conjunto al Ministerio de Relaciones Exteriores y al Centro de Respuesta a Incidentes Cibernéticos de Paraguay (CERT-PY) se aprueba en abril de 2017 por el Decreto 7052 el Plan Nacional de Ciberseguridad de Paraguay, el cual se plantea como un documento estratégico que sirve para coordinar las políticas públicas de ciberseguridad y generar un ambiente cibernético seguro, confiable y resiliente, fomentando la coordinación gubernamental, la cooperación pública-privada, la cooperación internacional como también, la elaboración de un marco legal óptimo que responda a las necesidades de las Tecnologías de la Información y Comunicación.

El Plan, cuenta con seis principios orientadores para la ciberseguridad en Paraguay, los cuales buscan impulsar un cambio cultural a nivel social y gubernamental basado en el uso responsable y seguro del ciberespacio. De igual manera, desde la agenda económica, buscan el progreso y la innovación de la nación, por medio de ambiente favorable para el crecimiento, desarrollo y competitividad para con las tecnologías. (Secretaría Nacional de Tecnologías de la Información y Comunicación [SENATICs], 2017). Para lo anterior, es fundamental la cooperación y coordinación entre el sector público y privado.

Cabe destacar que el Plan tiene una duración de tres años, es decir, cada tres años este será nuevamente evaluado por una comisión interdisciplinaria para ser actualizado y evolucionar al igual que evoluciona el ciberespacio. La idea es que el país paraguayo cuente con una estrategia congruente a las demandas de las personas, las organizaciones nacionales e internaciones como a las del sector público y privado.

Uruguay

La Agenda Uruguay Digital 2020 es el instrumento por el cual el gobierno busca un desarrollo tecnológico bajo el lema 'transformación con equidad'. La Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento, de la Presidencia de la República, es la entidad encargada de impulsar los objetivos y estrategias en base a los actores a quienes se busca beneficiar a través de medidas o políticas públicas. Frente a lo anterior, el Consejo para la Sociedad de Información, es el órgano que orienta los procesos de elaboración y priorización de las metas, así como el monitoreo y evaluación.

La elaboración de dicha agenda en el año 2016 significó el esfuerzo de distintos actores de la sociedad pertenecientes al sector público y privado, la academia, la sociedad civil organizada entendida en tecnología y la comunidad técnica (Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento de Uruguay [AGESIC], 2016), para integrar diversas iniciativas que permitan la transformación digital del país. Uno de los principales ejes de la Agenda Uruguay Digital 2020 es la inclusión y el uso sustentable de las tecnologías con el objetivo de ampliar los beneficios de la globalización a la mayor población posible, sobre todo a los sectores sociales que más dificultades tienen, por ejemplo, con la conexión a internet. La idea es generar el fortalecimiento de habilidades específicas para la ciudadanía en general, relacionadas con los dispositivos tecnológicos, la incorporación plena de la tecnología en sectores productivos y empresariales, como profundizar y fortalecer el vínculo ciudadanía-Estado. (AGESIC, 2016)

COMPARACIÓN ESTRATEGIAS NACIONALES DE CIBERSEGURIDAD

Tomando como marco de referencia los indicadores de ciberseguridad de la OECD analizamos las ENCS de los países del Cono Sur. En la tabla 2 se presentan los indicadores de ciberseguridad agrupados según sus fines, ya sean de: Protección, Cooperación y/o Estratégicos. La información relevada en cada caso será analizada en los párrafos posteriores.

Tabla 2: Análisis comparado de Estrategias Nacionales de Ciberseguridad.

	INDICADORES DE CIBERSEGURIDAD OECD / PAISES	ARG	BR	CHL	PAR	URU
Protección	Seguridad del gobierno	X	X	X	X	X
	Infraestructura de información críticas	X	X	X	X	X
	Monitoreo en tiempo real					
	Desarrollo de industrias de seguridad cibernética		X	X	X	
	Consideración de soberanía		X	X		
	Lucha contra el ciberdelito	X		X	X	X
	Respuesta	X	X	X	X	X
Cooperación	Cooperación Internacional	X	X	X	X	X
	Coordinación gubernamental - Multiagencia para un enfoque interinstitucional	X	X	X	X	X
	Cooperación público – privada	X	X	X	X	X
	Diálogo de multipartes interesadas			X	X	X
	Asociaciones con proveedores de servicios de internet (ISP)	X				
Estratégicos	Enfoque de política flexible	X	X		X	X
	Sensibilización	X	X	X	X	X
	Educación, Investigación y Desarrollo	X	X	X	X	X
	Resiliencia		X	X	X	
	Desarrollo de marcos de Identidad digital	X		X		X
	Políticas específicas para la protección de niños en línea	X			X	
	Respuesta de los valores fundamentales			X		

Fuente: elaboración propia, 2019.

Protección:

Se puede apreciar que los cinco países, en sus respectivas ENCS incluyen el indicador seguridad del Gobierno. En efecto, Argentina propone la elaboración de normas destinadas a incrementar los umbrales de seguridad, tanto en los recursos como en los sistemas que están relacionados con tecnologías informáticas del Sector Público Nacional. (Decreto N°13, 2016). Por su parte Brasil, cuenta con una agencia especializada para la seguridad del gobierno, esta es la Agencia Brasileña de Inteligencia, órgano encargado de proporcionar al presidente y a los ministros, información y análisis estratégico, necesarias para la toma de decisiones. (Agencia Brasileña de Inteligencia, s/f). Si bien, este órgano se encarga de cualquier tema que se relacione con la seguridad de gobierno, en los últimos años se ha puesto especial énfasis a las amenazas tecnológicas que pueden sufrir las estructuras gubernamentales a través del Centro de Investigación y Desarrollo para la Seguridad de las Comunicaciones, área de tecnología que desarrolla programas y herramientas para la transmisión segura de informaciones del Gobierno Federal. En cuanto a Chile, bajo el Decreto Supremo N°1 del año 2015 (Ministerio del Interior y Seguridad Pública, 2019), se establecieron normas técnicas sobre sistemas y sitios web de los Órganos de la Administración del Estado, las cuales están vigentes desde 2018 por el Instituto de Normalización (INN) para la Ciberseguridad, conducido por el Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT Chile).

Respecto a Paraguay, la Seguridad del Gobierno está coordinada por los agentes representantes o responsables de cada sección gubernamental. En este indicador, Paraguay apela a la correcta función de los altos cargos, teniendo conciencia situacional referente a la ciberseguridad. (SENATICs, 2017). Por último, Uruguay, plantea un trabajo conjunto entre los órganos gubernamentales a través de mesas ante incidentes cibernéticos. Cabe destacar que, para mayor control de los bienes tecnológicos que se utilizan en el sector público, se creó el Convenio Marco, el cual consiste en una modalidad de compras estatales en donde se seleccionan proveedores de bienes, obras y servicios a través de la Tienda Virtual de Agencia de Compras y Contrataciones del Estado. (AGESIC, 2019). La idea principal de este convenio es tener pleno conocimiento de las herramientas del sector gubernamental y un control estandarizado ante eventuales incidentes, además de garantizar menor costo, mayor eficiencia y calidad en el sector gubernamental.

Respecto a la protección de infraestructura de información crítica, de igual manera, los cinco países del Cono Sur incluyen en sus respectivas estrategias este indicador. Cada país cuenta con un equipo de tratamiento de ciberamenazas vinculados a los principales órganos de seguridad de Estado. Argentina cuenta con el Equipo de Respuesta a Incidentes de Seguridad Informática (CSIRT Argentina) dirigido por el Ministerio de Seguridad de la Nación. También cuenta con la Dirección Nacional de Infraestructura Críticas de Información y Ciberseguridad a cargo del Ministerio de Modernización, estas dos entidades que trabajan en conjun-

to para enfrentar incidentes cibernéticos que pongan en riesgo la información delicada para el normal funcionamiento del país. Además de contar con un CSIRT nacional, Argentina cuenta con el CSIRT de Buenos Aires, el cual se dedica a la asistencia y concientización de los ciudadanos y de los agentes de Gobierno de la capital de este país. En materia de infraestructura de información crítica, el país trasandino es el que ha desarrollado una contundente batería de leyes para responder a las necesidades cibernéticas (Disposición N°1, 2015), no es extraño si consideramos que los incidentes cibernéticos perpetrados en Argentina en los últimos años, han puesto en jaque las estructuras de seguridad de información crítica.

Lo que respecta a Brasil, este cuenta con el Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo[17] (CTIR Gov) conformado por Gendarmería Nacional, Policía Federal, Policía de Seguridad Aeroportuaria y Prefectura Naval. En un trabajo coordinado de las distintas entidades ya nombradas, tiene por objetivo coordinar la realización de acciones destinadas a la gestión de incidentes computacionales, ya sea de monitoreo, tratamiento y respuesta ante incidentes cibernéticos, en órganos gubernamentales. De igual forma, el CTIR Gov debe asesorar al Departamento de Seguridad de la Información del Gabinete de la Seguridad Institucional de la Presidencia de la República para la formulación de normativos y requisitos metodológicos en esta materia, velando por la seguridad de la información nacional. (CTIR Gov, 2019). Chile, por su parte, cuenta con el Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT Chile), bajo el alero del Ministerio del Interior y Seguridad Pública. En el caso de Chile, esta es la única entidad en manejar y coordinar los incidentes y vulnerabilidad dentro del Estado, esto, para poder priorizar y responder de forma canalizada las ciberamenazas que afectan a las infraestructuras críticas como también a la infraestructura de información crítica (Ministerio del Interior y Seguridad Pública, 2019). En la misma línea, Paraguay plantea que su Centro de Respuesta a Incidentes Cibernéticos (CERT-PY), sea la institución principal en la coordinación de las notificaciones de incidentes de seguridad que sufren las infraestructuras o redes paraguayas. El CERT-PY depende de la Secretaría Nacional de Tecnologías de la Información y Comunicación, y desde ahí, además del tratamiento de las ciberamenazas a las infraestructuras, promocionan la concienciación sobre los problemas de la seguridad informática. (Ministerio de Tecnologías de la Información y Comunicación, s/f). Por su parte Uruguay, cuenta con el Centro de Respuesta a Incidentes (CSIRT-UY) integrado por la Administración Nacional de Telecomunicaciones de Uruguay (ANTEL), conformando así el CSIRT de ANTEL. La función principal del CSIRT de ANTEL, aparte del tratamiento de las ciberamenazas, es la constante capacitación, coordinación y soporte en materia de seguridad informática tanto de los sistemas de red como del personal y de la comunidad, para así mejorar continuamente los servicios de internet. (CSIRT Antel, s/f). Para apoyar lo ya mencionado, Uruguay también cuanta con el Marco de Ciberseguridad (AGESIC, 2018), el cual suministra a la normativa nacional con normativas técnicas especializada para la protección de ciberamenazas.

Respecto al indicador monitoreo en tiempo real, el cual requiere de la detección inmediata a nivel operativo de las ciberamenazas mediante el establecimiento de Centros de Operaciones de Seguridad Cibernética (CSOC, por sus siglas en inglés), ninguno de los cinco países en estudio contempla en sus respectivas estrategias este indicador.

Por su parte, el desarrollo de industrias de seguridad cibernética está contemplado por tres de los cinco países analizados, Brasil, Chile y Paraguay. En estos tres países podemos ver los esfuerzos y hechos concretos respecto a este indicador. Brasil es el líder de este estudio en desarrollo de industrias de seguridad cibernética, ya que por medio de la Agencia Brasileña de Desarrollo Industrial, Brasil ha buscado el desarrollo constante de personal capacitado para enfrentar el desarrollo tecnológico e innovación, evidenciado en, por ejemplo, las Ciudades Inteligentes y o las energías renovables de Brasil, que requieren estrictamente de fuertes sistemas de seguridad cibernética para dar protección a nivel nacional e internacional. (Agencia para o desenvolvimiento da industria no Brasil, 2019). Paraguay por su lado, en su Plan Nacional de Ciberseguridad menciona que se debe fomentar modificaciones al marco legal para cumplir con la creación y funcionamiento de unidades especializadas de TIC y ciberseguridad, no obstante, no se especifica ningún lineamiento político para alcanzar dichas modificaciones legales. (Secretaría Nacional de Tecnologías de la Información y Comunicación, 2017). En tanto Chile, en su PNCS, este indicador solo se plantea como un esfuerzo que el país debe

[17] Traducción propia: Centro de Tratamiento y Respuesta a Incidentes Cibernéticos de Gobierno.

realizar en el medio y largo plazo. (Comité Interministerial Sobre Ciberseguridad, 2017).

El indicador consideración de Soberanía, tiene un importante enfoque militar y de defensa respecto al reconocimiento de las amenazas cibernéticas, exigiendo políticas que fomenten la seguridad desde esta perspectiva. En las estrategias de Brasil y Chile se especifica la militarización de la ciberseguridad a través de sus respectivas Política Nacional de Ciberdefensa. En el caso de Brasil, su Política Cibernética de Defensa, es establecida por medio de la ordenanza normativa N°3.389 (Lex Magister, 2019), la cual decreta que el Ministerio de Defensa de Brasil debe orientar las actividades de defensa y guerra cibernética a nivel estratégico, operativo y táctico. Para ello las ramas castrenses, Ejército, Fuerza Aérea y Marina, cada una tienen un Centro de Defensa Cibernética preparados para responder a incidentes, especialmente provenientes desde el exterior. En el caso de Chile, bajo la responsabilidad del Ministerio de Defensa Nacional, la Política de Ciberdefensa si bien tiene un enfoque militar, tiende más bien a una perspectiva de gestión de riesgos más que una respuesta relacionada a guerras cibernéticas. (Decreto N°3, 2018). El resto de los países en estudio, no especifican en sus respectivas estrategias la consideración de soberanía.

En cuanto a la lucha contra el ciberdelito, Argentina, Chile, Paraguay y Uruguay señalan en sus estrategias el tratamiento de dichos incidentes. En Argentina, la investigación y el procesamiento de los ciberdelitos y los cibercrímenes son llevadas a cabo por la Policía Federal, a través de la División de Delitos Tecnológicos. (BID & OEA, 2016). Por su parte Chile, para este tipo de delitos cuenta con la Brigadas Investigadoras del Cibercrimen de la Policía de Investigaciones (Policía de Investigaciones de Chile, 2019) y con el OS-9 de Carabineros de Chile. En cuanto a Paraguay, el Ministerio Público, a través de las distintas divisiones especializadas en delitos informáticos de la Policía Nacional enfrenta estos incidentes que se dan a nivel de ciudadanía. Dichas divisiones son: División Especializada Contra Delitos Financieros; División Especializada Contra Delitos Económicos; División Especializada Contra Violación de Derechos Intelectuales; División Especializada Contra Delitos Informáticos, División Especializada Contra el Lavado de Dinero y Financiamientos del Terrorismo; División Seguridad Bancaria; División Especializada Contra Hechos Punibles de la Prueba Documental; División Laboratorio y Estudios Periciales. (Dirección Contra Hechos Punibles Económicos y Financieros Policía Nacional, 2015) Lo que respecta a Uruguay, en su Agenda Uruguay Digital 2020, los delitos cometidos por las redes son tratados por el CERT-UY en conjunto a la Policía Nacional. Se tiene como objetivo adecuar y actualizar el marco normativo referente a la protección de datos personales, cibercrimen, e-residuos y protección e-consumidor, para ampliar el rango de tratamiento y solución ante estos ciberincidentes. Cabe señalar que la Organización Internacional de Policía Criminal (INTERPOL) hace periódicamente capacitaciones a la Policía Nacional de Uruguay para fortalecer las estrategias punitivas en esta materia a nivel nacional e internacional. (AGESIC, 2016).

Ante el indicador respuesta, los cinco países cuentan con sus respectivos Equipos de Respuesta a Incidentes de Seguridad Cibernética ya desarrollados en el indicador de Infraestructura de Información Crítica.

Cooperación:

La cooperación en sus distintas dimensiones sea internacional, intergubernamental y o cooperación público-privada es determinante para que un país cumpla con estándares mínimos de seguridad cibernética, pues la ciberseguridad no será efectiva si solo nutrimos un marco legal entorno a lo nacional, descuidando los quehaceres internacionales en materia cibernética, ya que, como lo hemos visto en capítulos anteriores, las ciberamenazas y todo lo que se relaciona con el ciberespacio, rompe fronteras.

El Convenio de Budapest, elaborado por el Consejo de Europa, el cual entró en vigor en el 2004, fue el primer y principal tratado internacional que se propuso aunar a los estados respecto delitos informáticos. Distintos países europeos como también variados países de otros continentes adhirieron al convenio para aplicar una política penal común en materia de cibercrimen. En efecto, de los cinco países analizados, Chile en el año 2017, Argentina y Paraguay en el año 2018 adhirieron y ratificaron el Convenio de Budapest haciendo con ello vinculante las decisiones pactadas en dicho convenio y la obligación de cumplir las políticas dispuestas para enfrentar los incidentes cibernéticos. (Council of Europe Portal, 2019).

Desde un panorama más regional, se cuenta con la Organización de Estados Americanos (OEA), organización internacional que apoya a los países Americanos, entre ellos Argentina, Brasil, Chile,

Paraguay y Uruguay en materia de ciberseguridad. A través del Comité Interamericano contra el Terrorismo la OEA apoya a los estados miembros en el desarrollo de capacidades técnicas, políticas e investigación (Organización de Estados Americanos, 2019). De igual modo, mejora la coordinación de intercambio de información y la cooperación entre los países americanos brindando asistencia a los CSIRT.

Ante la cooperación internacional, también se puede mencionar que los países en estudio han firmado importantes acuerdos bilaterales en el área de seguridad cibernética. En el caso de Argentina, en el 2017 firmó con España el Memorando de Entendimiento sobre Cooperación en Materia de Ciberseguridad (Ministerio de Modernización de la República de Argentina y Ministerio de Energía, Turismo y Agenda Digital del Reino de España, 2017), con el objetivo de impulsar estrategias comunes para la protección del ciberespacio. De igual modo, en el marco del G20 realizado en Argentina en el 2018, tras un acuerdo de asistencia técnica, Israel fue el país encargado de la protección cibernética de esta cumbre que reúne los principales líderes políticos y económicos del mundo, en la cual, la probabilidad de ciberataques era realmente una preocupación para el Estado argentino. (Dergarabedian, 2018).

En cuanto a Brasil, a través del Acuerdo de Intercambio y Protección Mutua de Información Clasificada, el gran país sudamericano estableció acuerdos bilaterales con España en el 2015 (Decreto N°9.273, 2018) y con Suecia en el 2018 (Decreto N°181, 2018), con la finalidad de proteger sus respectivas infraestructuras de información crítica, como también su soberanía a nivel cibernético, principalmente para enfrentar con mayor herramientas y conocimiento el ciberespionaje de las grandes potencias. Por su parte Chile, durante el 2018 estableció dos acuerdos bilaterales de ciberseguridad, uno con España y otro con Israel (Subsecretaría de Telecomunicaciones, 2018). Ambos acuerdos apuntan al intercambio de buenas prácticas en la aplicación de estrategias nacionales de seguridad cibernética. Específicamente la relación bilateral Chile-Israel, está destinada a robustecer el tratamiento técnico y cofinanciamiento de proyectos pilotos de infraestructura crítica de cara a la revolución tecnología de la quinta generación de tecnologías de telefonía móvil (5G).

Acerca de Paraguay, si bien en su Plan Nacional de Ciberseguridad se señala la importancia de la cooperación internacional, esta se ha mantenido a un nivel de cooperación con organismos supranacionales, principalmente en foros de ciberseguridad de la ONU y la OEA, por lo que no se han desarrollado acuerdos o cooperación bilateral. Ante esta deficiencia, se plantea como uno de los principales objetivos la cooperación multi y bilateral en materia de seguridad cibernética. (Secretaría Nacional de Tecnologías de la Información y Comunicación, 2017). Por último, en el caso de Uruguay, en el año 2017 se firmó el Acuerdo entre el Gobierno de la República Oriental del Uruguay y el Gobierno de la Federación de Rusia sobre Cooperación en Materia de Defensa (Ley N°19.607, 2018), en el cual se establecieron cooperación militar, de capacitación teórica y práctica, en temas de defensa y protección de información crítica.

Respecto a la coordinación gubernamental-Multiagencia para un enfoque interinstitucional, los cinco países plantean una coordinación y una cooperación entre los órganos gubernamentales. Argentina en su Estrategia Nacional de Ciberseguridad, cuenta con el Comisión de infraestructuras Tecnológica y Ciberseguridad permitiendo mayor coordinación en el trabajo de prevención y tratamiento de ciberamenazas (Argentina.gob.ar, 2019). En cuanto a Brasil, la función de coordinación la maneja el ya mencionado el CTIR Gov, el cual coordina la red formada por los órganos y las entidades gubernamentales (CTIR Gov, 2019). Por su parte Chile, CSIRT se hace cargo de la coordinación de los órganos del estado en conjunto al Comité Interministerial sobre Ciberseguridad. En este apartado, Chile plantea una Gobernanza para la eficiencia, calidad y buena orientación para la toma de decisiones (Comité Interministerial Sobre Ciberseguridad, 2017). Paraguay, por su lado, el CERT-PY es la principal entidad de coordinación, sin embargo, en el Plan Nacional de Ciberseguridad se platea reforzar la coordinación y cooperación intergubernamental creando procedimientos y líneas de acción específicas para el sector público, con canales de comunicación directo entre los Ministerios y Secretarías del Poder Ejecutivo. (Secretaría Nacional de Tecnologías de la Información y Comunicación, 2017). En el caso de Uruguay, cuenta con la Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento de Uruguay (AGESIC), esta agencia es la que coordina todos los asuntos en materia de ciberseguridad, incluida la coordinación entre los órganos gubernamentales del país. (AGESIC, 2016).

La cooperación público – privada es de suma importancia para la ciberseguridad, debido a que los incidentes cibernéticos, en su mayoría van dirigidos a instituciones privadas afectando principalmente al sector financiero. Es por lo anterior, que, en las respectivas ENCS de los cinco países en análisis se presenta este tipo de cooperación. Aunque dicha cooperación es hasta ahora incipiente, existen avances a destacar. Argentina, en su ENCS plantea elaborar, en conjunto al sector privado, políticas que resguarden la seguridad digital haciendo hincapié en las infraestructuras críticas del sector privado que son esenciales para el normal funcionamiento de las ciudades como del país (Resolución N°580, 2011). Brasil, por su parte, para la cooperación público-privada plantea crear un ecosistema digital por medio de la articulación de las empresas y la Institución de Ciencia y Tecnología. El órgano responsable de llevar a cabo esta articulación es el Gabinete de Seguridad Institucional de la Presidencia de la República con asesoramiento del Comité Gestor de la Seguridad de la Información. (Departamento de Segurança da Informação e Comunicações, 2015). En cuanto a Chile, cuenta con cooperación público-privada por medio de la Asociación Chilena de Empresas de Tecnología de Información, de la cual se obtienen conocimientos y asesoramientos en materia de cibernética desde el sector privado hacia el sector gubernamental. (Asociación Chilena de Empresas de Tecnología de Información, 2019).

Respecto a Paraguay, la cooperación público-privada se hace por medio de asistencia técnica y teórica de operadores privados, sobre todo a las infraestructuras de críticas, viéndose reflejado en un constante trabajo en el CERT-PY. (Secretaría Nacional de Tecnologías de la Información y Comunicación, 2017). Uruguay por su lado, en su Agenda Uruguay Digital 2020, apunta la innovación del sector privado, trabajando en conjunto al AGESIC, entregando herramientas de tecnologías, capacitaciones y programas de formación al sector privado. (AGESIC, 2016). Cabe destacar que, dentro de estos proyectos, Uruguay contempla potencia la ciberseguridad en las micros, pequeñas y medianas empresas.

Ante el indicador diálogo multipartes interesadas, Chile, Paraguay y Uruguay, en sus respectivas estrategias plantean objetivos que recogen los conocimientos de los diversos actores a los que compromete la ciberseguridad. En Chile, el CSIRT constantemente está solicitando ayuda de expertos en seguridad cibernética, ya sea del sector privado, la academia como la sociedad civil para nutrir y ampliar la capacidad de respuesta ante factores de riesgo cibernéticos. Lo anterior se sustenta en la Alianza Chilena de Ciberseguridad, entidad integrada por las diversas partes interesadas en el desarrollo y promoción de la ciberseguridad. (Alianza Chilena de Ciberseguridad, 2019).

Dicha alianza aúna no solo actores nacionales en la materia, sino también tiene contactos internacionales que permiten mayor cooperación con las autoridades. Por su parte Paraguay, cuenta con la Comisión Nacional de Ciberseguridad, instancia donde se refuerzan las relaciones de coordinación, colaboración y cooperación entre las partes interesadas en la ciberseguridad, incluyendo al Estado, sector privado, la academia y la sociedad civil. (Secretaría Nacional de Tecnologías de la Información y Comunicación, 2017). Uruguay por su lado, a través del Centro Nacional de Operación de Ciberseguridad recoge las opiniones y estudios que las diversas partes quieren y pueden aportar en materia de seguridad cibernética e infraestructuras críticas. (AGESIC, 2016). Cabe destacar que los tres países tuvieron la precaución de incluir en la elaboración de sus ENCS las opiniones, sugerencias y críticas de las partes interesadas, por medio de consultas ciudadanas.

El indicador asociaciones con proveedores de servicios de internet, muestra el poco compromiso de cuatro de los cinco países estudiados. Argentina es el único país que establece en su estrategia mecanismo para facilitar el intercambio de información entre el sector gubernamental y los proveedores de internet, sobre todo ante situaciones de fraudes, ciberdelitos o cibercrimen. (Leiva, 2015).

Estrategia:
En todo ámbito, donde es necesaria la toma de decisiones rápida e informada, el constante aprendizaje, retroalimentación y mejoramiento, son esenciales para optimizar recursos y tiempo. Precisamente, es lo anterior lo que busca un enfoque de política flexible en la ciberseguridad. Cuatro de los cinco países estudiados trabajan este enfoque en sus ENCS. Argentina, para fomentar el estudio y la retroalimentación, y que esto repercuta en la buena utilización de los recursos, elabora anualmente un informe de la situación de la ciberseguridad del país. Dicho informe es de carácter público y bajo transparencia para mostrar los costes de esta materia. Brasil por su lado, anualmente mide el nivel de madurez de los principales órganos gubernamentales que trabajan, desarrollan y promo-

cionan la ciberseguridad, estableciendo comparaciones respecto a años anteriores, verificando cuales han sido las metas cumplidas y qué aspectos están por debajo de lo que el país necesita.

En la ENCS de Brasil, se plantea, para mayor control, establecer un mecanismo de mapeo sistemático de los activos que afecten directamente en la continuidad de la misión del Estado y la sociedad que compone la infraestructura crítica de la información. Las entidades encargadas de la medición de madurez como de establecer el mecanismo de mapeo es el Gabinete de Seguridad Institucional de la Presidencia de la República en conjunto al Comité Gestor de la Seguridad de la Información. (Departamento de Segurança da Informação e Comunicações, 2015). En cuanto a Paraguay, en el Plan Nacional de Ciberseguridad se plantea que este mismo será revisado y actualizado cada tres años o cuando sea necesario, ya que se comprende la constante evolución de las amenazas cibernéticas como de las Tecnologías de la Información y la Comunicación. La revisión y actualización dependerá del Coordinador Nacional de Ciberseguridad. (Secretaría Nacional de Tecnologías de la Información y Comunicación, 2017). En el caso de Uruguay, se elabora un constante diagnóstico de la Agenda Digital Uruguay para actualizar las temáticas de la misma agenda e ir ampliando como a su vez precisando la ciberseguridad. (AGESIC, 2016).

Respecto al indicador sensibilización, los cinco países cumplen con estrategias que fortalecen a la población en el uso responsable de las tecnologías e internet. En el caso de Argentina, en su ENCS se promueve la concientización en base a los riesgos que conlleva el uso de medios digitales y tecnologías de la información y comunicación. La concientización del país trasandino está dirigida al sector público, las organizaciones de gobierno, al público en general, como también al sector privado y a las relaciones público-privado. El más reconocido programa argentino que se dedica a la sensibilización y concientización en materia de seguridad informática es el programa "Con vos en la Web". (Argentina.gob.ar, 2019). Dicho programa es dirigido por la Dirección Nacional del Sistema Argentino de Información Jurídica, dependiente del Ministerio de Justicia y Derechos Humanos de la Nación, y tiene por objetivo concientizar a las personas en el uso responsable de las Tecnologías de la Información y Comunicación, dar herramientas para disminuir los riesgos cibernéticos manifestados principalmente en las redes sociales.

El programa "Con vos en la Web" está pensado especialmente para padres, profesores y o adultos significativos de menores. (Argentina.gob.ar, 2019). Brasil por su lado, por medio de los agentes responsables de la Seguridad Cibernética de la Administración Pública Federal, se promueven campañas de concientización para la sociedad, enfocado principalmente en los niños, niñas y jóvenes. (Departamento de Segurança da Informação e Comunicações, 2015). En el caso de Chile, se cuenta con el programa "Ciudadanía Digital" dirigido por el Ministerio de Educación. Dicho programa consiste en un conjunto de medidas que posibilitan y desarrollan el conocimiento, habilidades y actitudes de niños, niñas, jóvenes y adultos, para un desenvolvimiento responsable en el ciberespacio. (Internet Segura y Ciudadanía Digital, 2019).

Este programa se levanta sobre las bases de los derechos digitales, para el respeto de los valores fundamentales de los niños, niñas y jóvenes. Respecto a Paraguay, en su ENCS se plantea la incorporación progresiva de prácticas que promocionen la ciberseguridad por un periodo indeterminado o hasta que se genere una cultura en torno a la seguridad cibernética. (Secretaría Nacional de Tecnologías de la Información y Comunicación, 2017). Por su parte Uruguay cuenta con el Plan Ibirapitá el cual está destinado a la inclusión de los jubilados a la era digital por medio de talleres, entrega de dispositivos tecnológicos como tablet, curso para el manejo de los dispositivos y manejo de internet. (Plan Ibirapitá, 2019).

En cuanto al indicador educación, investigación y desarrollo, los países del Cono Sur han puesto todos sus esfuerzos en este tema, cumpliendo cada estado con este indicador. No obstante, los objetivos planteados y medidas implementadas son distantes unas a otras, mostrando cómo algunos países tienen una educación en materia cibernética más robusta en comparación de otros países en análisis. En el caso de Argentina, se plantea un constante asesoramiento a nivel educacional y técnico ante incidentes informáticos en órganos gubernamentales que lo requieran o así lo soliciten.

De igual modo, a un nivel ciudadano, el país trasandino cuenta con el "Internet Sano", programa que enseña de forma didáctica a navegar e interactuar en internet, por medio de videos explicativos que logran evidenciar las situaciones de riesgos como también las formas en las que se debe actuar ante posibles ciberamenazas o ciberdelitos. (Jefatura de Gabinete de Ministros, 2019). Para reforzar la educación, la investigación y el desarrollo, Argentina, a

través del Instituto Nacional de Administración Pública, se dedica a la formación profesional de funcionarios y empleados públicos en sistemas de red y seguridad de la información. (Instituto Nacional de Administración Pública, 2019).

Brasil por su parte, en materia de educación cuenta con convenios universitarios para desarrollar a futuro profesionales en ciberseguridad, tanto en el área técnica como en la formulación de políticas públicas en torno a la seguridad, responsabilidad y tratamiento de ciberincidentes. (Departamento de Segurança da Informação e Comunicações, 2015). En el caso de Chile, cuenta con dos programas educativos para orientar el autocuidado y prevención en el ambiente digital orientado a diferentes rangos etarios. El programa "Enlace" tiene como finalidad entregar conocimientos y herramientas a los adultos responsables de menores para que puedan acompañar y formar a los niños, niñas y jóvenes desde un enfoque responsable y seguro en el ciberespacio. (Enlaces, 2019).

En tanto, el programa "Internet Segura" apuesta por la orientación de escuelas y liceos, desde una mirada pedagógica, para formar ciudadanos conscientes en sus derechos y deberes digitales, es por ello, que este programa está destinado a escolares de educación básica y media de los distintos establecimientos educaciones de Chile, ya sean municipales, particular subvencionado y particulares. (Internet Segura y Ciudadanía Digital, 2019).

En la misma línea educacional, pero desde un nivel de post título, Chile cuenta con la Academia Nacional de Estudios Políticos y Estratégicos del Ministerio de Defensa. Dicha academia imparte diplomados, licenciaturas y magister en el área de defensa, estrategia y ciberseguridad, tanto para personas pertenecientes a las ramas castrenses como para civiles. (Academia Nacional de Estudios Políticos y Estratégicos, 2019). Cabe destacar, que las universidades chilenas también cuentan con espacio para fomentar y fortalecer la ciberseguridad, siendo uno de los más reconocidos es el CLCERT. (Clcerte, 2019).

Por su parte Paraguay, imparte programas y cursos específicos en todos los niveles de enseñanza, desde básica a la superior, para incentivar la ciberseguridad y el buen uso de las Tecnologías de la Información y Comunicación. (Secretaría Nacional de Tecnologías de la Información y Comunicación, 2017). Por último, Uruguay cuenta con el programa "Jóvenes a Programar", el cual apunta a la capacitación e inserción laboral de jóvenes programadores de las Tecnologías de la Información y Comunicación a empresas privadas. (Plan Ceibal, 2019). Para fortalecer la proactividad en el conocimiento, este país ha elaborado el Sistema Nacional de Repositorio, el que permite compartir y consultar trabajos y artículos científicos de producción nacional en diversos temas y áreas, incluida la seguridad cibernética. (Timbó, 2019).

El indicador resiliencia, entendida como la capacidad de los sistemas de red gubernamentales y privados de estar preparados o recuperarse ante ciberincidentes, es uno de los indicadores claves para ver la efectividad de la ciberseguridad de un país. Brasil, Chile y Paraguay, contemplan en sus respectivas estrategias la resiliencia como fundamental para el normal funcionamiento del país y amortiguar los posibles daños para las estructuras estatales, privadas y ciudadanas. Brasil de cara a lo anterior, mantiene como objetivo en su estrategia establecer mecanismos para el mapeo sistemático de daños de infraestructuras, justamente para tener respuesta de recuperaciones rápidas y efectivas, damnificando lo menos posible las estructuras. (Departamento de Segurança da Informação e Comunicações, 2015).

Chile por su parte, cuenta con la Ley 20.478 sobre la Recuperación y Continuidad en Condiciones Críticas y de Emergencia del Sistema Público de Telecomunicaciones, la cual, si bien indica la recuperación rápida de los sistemas en instancias de catástrofes naturales, en los últimos años se han modificado como agregado artículos para incluir la recuperación de los sistemas a nivel tecnológico. Los artículos 39 A y 39 B de dicha ley se especifican sobre la recuperación de las Infraestructuras Críticas de Telecomunicaciones a través de la coordinación de los órganos encargados de las infraestructuras críticas como también un plan de resguardo de dichas infraestructuras post ciberincidentes a partir de las decisiones de la Subsecretaría de Telecomunicaciones. (Ley Nº20478, 2010).

En el caso de Paraguay, en su Pan Nacional de Ciberseguridad, si bien se menciona que las infraestructuras críticas son resilientes antes las amenazas cibernéticas y que cumplen con garantizar la estabilidad de los servicios esenciales, no se presenta una mayor profundización del tema, no mencionando la entidad a cargo de la resiliencia de los órganos gubernamentales, ni algún tipo de medida, ley o política pública que se refiera al tema. (Secretaría Nacional de Tecnologías de la Información y Comunicación, 2017).

Frente a los indudables avances tecnológicos, los marcos de identidad digital son una necesidad tanto para el Estado como para los ciudadanos para optimizar recursos ante los trámites que se soliciten desde el área gubernamental. El indicador desarrollo de marcos de identidad digital, el cual básicamente trata de la identidad en línea, es recogido por tres de los cinco países en estudio. Argentina, Chile y Uruguay, cada país cuenta con un sistema de identidad digital el cual establece la autenticación en línea, permitiendo el libre acceso a documentos personales y servicios de gobierno de manera remota, en tiempo real y de cualquier dispositivo que cuente con acceso a internet.

En el caso de Argentina, el Sistema de Identidad Digital (SID), la autenticación se hace biométricamente, es decir, el acceso depende del reconocimiento facial de quien solicita ingresar. El SID depende del Ministerio del Interior, Obras Públicas y Vivienda, en conjunto a la Secretaría de Modernización. (Argertina.gob.ar, 2019) Chile por su parte, trabaja por medio de la Identidad Digital Única, perteneciente al programa Gobierno Digital.

La Identidad de Digital Única se hace mediante la "Clave Única", instrumento por el cual se digitaliza la identificación de las personas naturales, permitiendo solo de esta manera, el acceso a los servicios públicos vía web. El Estado chileno paulatinamente ha implementado este instrumento para los servicios de gobierno, fijándose el plazo para el 2020 todos los trámites y servicios gubernamentales se hagan en esta modalidad. Cabe destacar que, aparte de la Identidad Digital Única, Chile también cuenta con otros programas que facilitan los servicios digitales gubernamentales tales como: programa Cero Filas y programa Cero Papel. El Consejo Ejecutivo de Modernización de Estado es el encargado del diseño de los programas nombrados. (Gob digital, 2018).

Uruguay por su lado, este indicador lo desarrolla por medio de ID Uruguay, el cual forma parte del Gobierno Electrónico impulsado en los últimos años. El ID Uruguay es el nuevo sistema de gobierno que permite, a través de una única cuenta, acceder a todos los servicios del Estado. Tener la ID Uruguay no es obligatorio sino, más bien puede obtenerla cualquier persona en el momento que lo desee, y no se exige como requisito para los servicios del Estado. La entidad a cargo de la ID Uruguay es la AGESIC. (AGESIC, 2019).

El creciente acceso a las tecnologías y a internet trae consigo la preocupación de la población más vulnerable del ciberespacio, los niños y niñas, que sin mayor conocimiento a lo que se exponen en la red, son blanco fácil para personas que, desde el otro lado de la pantalla, quieren causar daño. El indicador políticas específicas para la protección de niños en línea, justamente quiere enfrentar las inseguridades que los menores viven en esta dimensión, por ello, es fundamental la formulación de políticas específicas que se encarguen de sucesos tales como ciberacosos, ciberbullying, entre otros. De los cincos países del Cono Sur analizados, solo dos tienen trabajos referentes a este tema. Argentina trabaja por medio de Equipo Niñ@s, el cual brinda asesoramiento y acompañamiento las 24 horas, todos los días del año a niñas, niños y adolescentes víctimas de acoso sexual mediante el uso de internet (Crooming), víctimas de pornografía infantil, víctimas de explotación sexual y víctimas de explotación sexual comercial infiltrada en viajes y turismo. El Equipo Niñ@s desarrolla acciones de sensibilización, prevención y capacitación en todo el país a los actores del área de turismo, educacional, salud, seguridad y funcionarios de los tres poderes del Estado. Es importante resaltar que Equipo Niñ@s cuenta con una línea gratuita y correo para las denuncias en esta materia. (Ministerio de Justicia y Derechos Humanos, 2019).

En cuanto a Paraguay, el Ministerio Público, en conjunto a la Policía Nacional y la cooperación del Centro Nacional para Niños Desaparecidos y Explotados, investigan casos de explotación sexual de niñas y niños contactados por redes sociales como también la exhibición de imágenes y oferta de menores de edad por vía web. Por otro lado, frente a los casos de cyberbullying y ciberacoso, la Policía Nacional cuenta con unidades especializadas para el tratamiento minucioso de estos temas (Ministerio Público, 2019), ya que, al ser cometidos estos delitos informáticos a través de tecnologías e internet, requieren de un abordaje particular, desde la investigación, recolección, manejo de evidencia y prueba digital.

Ante los indudables riesgos de la web, los países tienen la obligación de resguardar la seguridad de las personas en el ciberespacio, incluso de sus propios Estados, pues, en lo inmediato, son los ciudadanos los que no cuentan con las herramientas ni conocimientos idóneos para enfrentar la vulneración de su desarrollo personal en internet. El último indicador de respuesta de valores fundamentales precisamente apunta a que las personas puedan realizar sus actividades personales, sociales y comunitaria vía web

respetándoles la privacidad, la libertad de expresión y el libre flujo de información de cada persona.

Si bien con este indicador se busca que ningún agente quebrante los derechos de quien utiliza la web, está destinado esencialmente a que los Estados no coarten la libertad de sus ciudadanos en la dimensión cibernética. De los cinco países en análisis, solo uno en su ENCS hace énfasis en este tema. Chile en su PNCS(Comité Interministerial Sobre Ciberseguridad, 2017), plantea que los objetivos propuesto como las medidas ya concretadas en ciberseguridad, su diseño y ejecución tienen un enfoque de derechos fundamentales, atendiendo su carácter universal e indivisible y sobre la base que el ciberespacio es un ambiente donde las personas cuentan con los mismos derechos que en el mundo físico. Para que realmente se respeten los valores fundamentales, el Ministerio de Justicia y Derechos Humanos de Chile es el encargado de velar por el cumplimiento, actualización y adecuación técnica de la legislación a los desafíos que trae el desarrollo tecnológico.

El indicador monitoreo en tiempo real es el indicador que ningún país en observación cumple. En base a la definición de este indicador, se entiende que para que este se concrete, se requieren de esfuerzos concentrados en el sector público, principalmente en la administración de las infraestructuras gubernamentales, no obstante, dichos esfuerzos no se refieren precisamente a una coordinación realizada por medio de una reunión o foros en los cuales se lleguen acuerdos entre los distintos representantes de estructuras gubernamentales.

Si bien esas instancias son necesarias, los esfuerzos que solicita el monitoreo en tiempo real apuntan al establecimiento de Centros de Operaciones de Seguridad Cibernética, los cuales logren administrar y coordinar técnicamente las infraestructuras críticas estatales. Por lo tanto, se entiende que, para los cinco países en análisis, es mucho más complicado ejecutar este tipo de Centros de Operaciones de Seguridad Cibernética propuesto por la OECD, puesto que su desarrollo implicaría un uso de recursos monetarios y humano importante. Más aún si consideramos que recién en los últimos años se busca invertir en capital humano apto para cargos que requieren de conocimiento cibernético y de toma de decisiones en momentos de crisis.

De igual forma, llama la atención que el indicador Asociaciones con Proveedores de Servicios de Internet evidencia vacíos. Así, Brasil, Chile, Paraguay y Uruguay, en sus respectivas ENCS, no se han planteado objetivos para generar cooperación con las empresas que prestan servicios a la ciudadanía, a las grandes instituciones privadas y gubernamentales. Los Proveedores de Servicios de Internet son actores fundamentales en el contexto de globalización en donde las nuevas tecnologías conectadas a la red de internet están presentes en las mayorías de trabajos, actividades y quehaceres en general del ser humano. De ahí entonces, que es fundamental generar lazos o, derechamente cooperación, entre estas empresas que brinda la conexión a internet a cientos de usuarios, puesto que son ellos quienes pueden entregar información importante respecto a las amenazas a la web.

En ese sentido, el incumplimiento por la mayoría de los países en análisis demuestra que la cooperación interna, entre las instituciones privadas e instituciones gubernamentales no ha sido prioridad para las estrategias, y que los avances que existen hasta ahora, no consideran una coordinación entre estos sectores la cual apunte a alcanzar una meta de carácter nacional como lo es la protección de los usuarios de internet, por el contrario, la cooperación existente se mantiene a nivel teórica la cual se basa en compartir conocimientos y asesoramientos, pero no en la acción concreta de coordinar a las instituciones.

Respecto al área estratégica, el indicador menos cumplido por los países en análisis es Respuesta de valores fundamentales, ya que solo Chile contempla los valores privacidad, libertad de expresión y el libre flujo de información promovidos por la OECD. Para cumplir con el respeto de los valores fundamentales, se requiere que las políticas elaboradas e implementadas en materia de ciberseguridad tenga un enfoque en donde el respeto al ser humano no se trance, permitiendo el normal desarrollo de este en el mundo cibernético. Esto implica que, el Estado chileno debe garantizar, que a las personas, se nos respete nuestra privacidad, velando por la protección de los datos personales, datos financieros y cualquier documento o imagen que exponga información personal delicada. De igual forma, el Estado debe garantizar la libertad de expresión, entendida esta también como un elemento fundamental de Derechos Humano. Por último, el Estado debe garante del libre flujo de información, para que los diversos sectores y actores de la sociedad tenga la posibilidad de manifestar, bajo respeto, sus pen-

samientos e intereses, como también para permitir el libre acceso a las personas a informase desde múltiples fuentes, considerando que el libre flujo de información es un componente esencial para la democracia.

CONCLUSIÓN

Las ciberamenazas son vulnerabilidades propias del desarrollo tecnológico, de internet y la era de la globalización, estas nuevas amenazas ejecutadas desde y en el ciberespacio se han manifestado en algunos países latinoamericanos, afectando muchas veces el normal funcionamiento de los servicios y otras actividades de quienes utilizan internet. Es por ello, que la ciberseguridad es una necesidad real para la seguridad de los países, tanto para proteger sus infraestructuras críticas del sector gubernamental y privado, como también para proteger y permitir el desenvolvimiento normal y cotidiano de miles de personas conectadas a la red.

Estas amenazas cibernéticas afectan de manera indiscriminada, teniendo un alcance global, por lo que la sociedad internacional, específicamente los organismos internacionales se han pronunciado al respecto para aportar ayuda a los países, tanto en el diseño y lineamientos de sus políticas públicas de ciberseguridad, como en la asistencia técnica. De ahí la importancia del estudio de las políticas, o derechamente, de las ENCS de Argentina, Brasil, Chile, Paraguay y Uruguay teniendo como marco de referencia los indicadores de ciberseguridad, una de las organizaciones más influyentes en el escenario internacional que vela por la promoción de una cultura de seguridad cibernética con un enfoque integral, como es la Organización para la Cooperación y el Desarrollo Económico.

Las ENCS han avanzado en algunos temas propuestos por la OECD (2012), tales como: seguridad del gobierno, infraestructura de información crítica, cooperación internacional, coordinación gubernamental – Multiagencia para un enfoque interinstitucional, cooperación público-privada, sensibilización y educación, investigación y desarrollo. De igual modo, se da cuenta que la mayoría de los países concentran sus esfuerzos en el apartado cooperación, específicamente en el indicador cooperación internacional, ya que desde ahí se han levantado y realizado concretas alianzas que ayudan a mejorar las relaciones bilaterales y multilaterales en materia de seguridad cibernética.

Sin embargo, si bien el estudio de caso comparativo muestra que el resto de los indicadores del apartado cooperación son cumplidos por Argentina, Brasil, Chile, Paraguay y Uruguay al incluir objetivos en sus respectivas ENCS, el análisis posterior nos arroja que dichos indicadores solo son esfuerzos principalmente narrativos, ya que implican acuerdos, asesorías y difusión de conocimientos, siendo que, lo que se espera, es que logre una coordinación real entre las partes cooperantes para sentar las bases de una ciberseguridad efectiva en cada país.

Entre los indicadores de ciberseguridad que quedan pendientes, existe monitoreo en tiempo real, asociaciones con proveedores de servicios de internet y respuesta de los valores fundamentales. El poco compromiso por parte de la mayoría de los países estudiados en estos indicadores, se problematizan más aún cuando consideramos que los indicadores monitoreo en tiempo real y respuesta de valores fundamentales son caracterizados como relevantes y prioritarios.

Se puede concluir, que Chile es el país que cumple con la gran mayoría de los indicadores de ciberseguridad de la OECD, incluso con aquellos de carácter prioritarios definidos por dicha organización. Le sigue Paraguay, que cumple la mayoría de los indicadores, no obstante, solo con dos de los cuatro indicadores relevantes.

Los casos más preocupantes son Argentina, Brasil y Uruguay, ya que no han logrado elaborar sus respectivas ENCS en base a las exigencias nacionales e internacionales que la ciberamenazas traen consigo para la seguridad cibernética. Sin embargo, cabe destacar el caso de Brasil, que, si bien no registra una cantidad de cumplimientos significativos de los indicadores trabajados, al menos en los que marca cumplimiento, en general, son materializados y no se quedan en el nivel narrativo.

Así, el camino a seguir para diseñar e implementar políticas que permitan enfrentar el incremento de las ciberamenazas es aún largo y requiere de serios compromisos políticos así como de acuerdos transversales que incluyan a la empresa privada y la sociedad civil. Tarea que por ahora es esquiva en la región.

REFERENCIAS

Academia Nacional de Estudios Políticos y Estratégicos. (2019). *¿Quiénes somos?* Recuperado de https://www.anepe.cl/portada-quienes-somos/

Agência Brasileira de Inteligência. (s.f.). *O que é, O que faz, Como faz.* Recuperado de http://www.abin.gov.br/institucional/a-abin/

Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento de Uruguay. (2016). *Agenda Uruguay 2020.* Recuperado de https://www.agesic.gub.uy/innovaportal/file/6122/1/agenda-uruguay-digital---enero-final.pdf

Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento. (2019). *Tienda virtual de agencia de compras y contrataciones del Estado.* Recuperado de https://www.comprasestatales.gub.uy/tienda/

Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento. (2018). *Marco de ciberseguridad.* Recuperado de https://centroderecursos.agesic.gub.uy/web/seguridad/wiki/-/wiki/Main/Marco+de+Ciberseguridad

Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento. (2019). *Firma electrónica.* Recuperado de https://www.agesic.gub.uy/innovaportal/v/6726/38/agesic/que-es.html?idPadre=6723

Agencia para o Desenvolvimento da Industria no Brasil. (2019). *Proyectos.* Recuperado de https://abdi.com.br/inovacao

Alianza Chilena de Ciberseguridad. (2019). *¿Quiénes somos?* Recuperado de https://www.alianzaciberseguridad.cl/#somos

Arias, J. (25 de junio de 2011). Brasil sufre un ciberataque a gran escala. *El País*. Recuperado de https://elpais.com/diario/2011/06/25/internacional/1308952808_850215.html

Asociación Chilena de Empresas de Tecnología de Información. (2019). *¿Quiénes somos?* Recuperado de http://www.acti.cl/quienes_somos/

Banco Interamericano de Desarrollo & Organización de Estados Americanos. (2016). *Ciberseguridad ¿Estamos preparados en América Latina y el Caribe?* Recuperado de https://www.casede.org/index.php/biblioteca-casede-2-0/seguridad/ciberseguridad/468-ciberseguridad-estamos-preparados-en-america-latina-y-el-caribe/file

Borghello, C., & Temperini, M. (2013). Ciberseguridad nacional argentina: Cracking de servidores de la administración pública. En Simposio de Informática y Derecho. *Jornadas Argentinas de Informática, 42.*

Centro Nacional de Respuesta a Incidentes de Seguridad Informática. (2015). *Estadísticas de incidentes primer semestre 2015.* Recuperado de https://www.gub.uy/centro-nacional-respuesta-incidentes-seguridad-informatica/datos-y-estadisticas/estadisticas/estadisticas-de-incidentes-del-primer-semestre-de-2015

Centro Nacional de Respuesta a Incidentes de Seguridad Informática. (2016). *Estadísticas de incidentes de CERTUY en 2016.* Recuperado de https://www.gub.uy/centro-nacional-respuesta-incidentes-seguridad-informatica/datos-y-estadisticas/estadisticas/estadistica-de-incidentes-de-certuy-en-2016

Clcerte (2019). *Nosotros.* Recuperado de https://www.clcert.cl/nosotros/

Comité Interministerial sobre Ciberseguridad. (2017). *Política nacional de ciberseguridad.* Recuperado de https://www.ciberseguridad.gob.cl/media/2017/05/PNCS-CHILE-FEA.pdf

Con vos en la web (2019). Recuperado de https://www.argentina.gob.ar/justicia/convosenlaweb

Council of Europe Portal. (2019). *Chart of signatures and ratifications of treaty 185.* Recuperado de https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=S5PssuRE

CSIRT ANTEL. (s.f.). *¿Qué hace el CSIRT de ANTEL?* Recuperado de https://www.csirt-antel.com.uy/que_hace

CTIR Gov. (2019). *Acerca CTIR Gov.* Recuperado de https://www.ctir.gov.br/es/

Decreto No.181-18. (2018). *Aprova o texto do Acordo entre a República Federativa do Brasil e o Reino da Suécia sobre Troca e Proteção Mútua de Informação Classificada, assinado em Estocolmo, em 3 de abril de 2014.* Camara Dos Deputados. Brasil.

Decreto No.13-16. (2016). *Estructura del Ministerio de Modernización y del Ministerio de Defensa. Información Legislativa.* Buenos Aires, Argentina. Recuperado de http://servicios.infoleg.gob.ar/infolegInternet/anexos/255000-259999/257556/texact.htm

Decreto No.3-18. (2018). Ministerio de Defensa Nacional aprueba Política de Ciberdefensa. *Diario Oficial de la República de Chile.* Santiago de Chile, Chile. Recuperado de https://www.diariooficial.interior.gob.cl/publicaciones/2018/03/09/42003/01/1363153.pdf

Decreto No.9.273-15. (2015). *Promulga o acordo entre a República Federativa do Brasil e o Reino da Espanha relativo à troca e proteção mútua de informações classificadas, firmado em Brasília, em 15 de abril de 2015.* Camara Dos Deputados. Brasil. Recuperado de https://www2.camara.leg.br/legin/fed/decret/2018/decreto-9273-31-janeiro-2018-786134-norma-pe.html

Departamento de Segurança da Informação e Comunicações. (2015). *Estratégia de segurança da informação e comunicações e de segurança cibernética da administração pública federal 2015 – 2018.* Recuperado de http://dsic.planalto.gov.br/legislacao/4_Estrategia_de_SIC.pdf/view

Dergarabedian, C. (2018). G20: el Gobierno refuerza la ciberseguridad de la cumbre con ayuda de Israel. *iProfesional.* Recuperado de https://www.iprofesional.com/tecnologia/281619-buenos-aires-costa-salguero-macri-G20-el-Gobierno-refuerza-la-ciberseguridad-de-la-cumbre-con-ayuda-de-Israel

Díaz, J. R. (2016). Ciberamenazas: ¿El terrorismo del futuro? bie3: *Boletín ieee*, *3*, 541-561.

Dinatale, M. (2018). Los hackeos aumentaron un 700% en Argentina y el gobierno aceleró el comando de ciberseguridad. *Infobae.* Recuperado de https://www.infobae.com/politica/2018/02/11/los-hackeos-aumentaron-un-700-en-argentina-y-el-gobierno-acelero-el-comando-de-ciberseguridad/

Dirección Contra Hechos Punibles Económicos y Financieros Policía Nacional. (2015). *Divisiones especializadas.* Recuperado de http://www.delitoseconomicos.gov.py/index.php/dependencias/sede-central

Disposición No.1. Aprueba la política modelo de seguridad de la información. *Normativa-ciberseguridad*. (2015). *Información Legislativa.* Recuperado de http://servicios.infoleg.gob.ar/infolegInternet/anexos/240000-244999/242859/norma.htm

El Ciudadano. (2017). *Chile sería el quinto país con más ciberataques en todo américa.* Recuperado de https://www.elciudadano.com/ciencia-tecnologia/chile-seria-el-quinto-pais-con-mas-ciberataques-en-toda-america/03/22/

Enlaces. (2019). *¿Quiénes somos?* Recuperado de http://www.enlaces.cl/sobre-enlaces/quienes-somos/

Fernández, A. V., & Rodríguez, J. M. C. (2017). Análisis de las ciberamenazas. *Cuadernos de Estrategia*, *185*, 97-138.

Frieiro, R., Pérez, P. y Pascual, X. (2017). ¿Qué impacto ha tenido el ciberincidente de WannaCry en nuestra economía? *Cyber Risk, 6,* 1-32.

Gobierno de España. Ministerio de Defensa, Secretaría General Técnica. (2014). *Documentos de seguridad y defensa 60. Estrategia de la información y seguridad en el ciberespacio.* Recuperado de https://www.uma.es/foroparalapazenelmediterraneo/wp-content/uploads/2014/07/dsegd_60.pdf

Gob Digital. (2018). *Instructivo presidencial de transformación digital.* Recuperado de https://digital.gob.cl/instructivo/identidad-digital

Instituto Nacional de Administración Pública. (2019). *Portal de capacitación.* Recuperado de https://capacitacion.inap.gob.ar/

Internet Segura y Ciudadanía Digital. (2019). *Comunidad educativa.* Recuperado de http://www.internetsegura.cl/comunidad-educativa/

Internet Segura y Ciudadanía Digital. (2019). *Orientaciones de ciudadanía digital para la formación ciudadana.* Recuperado de http://www.internetsegura.cl/comunidad-educativa/orientaciones-ciudadania-digital/

Jefatura de Gabinete de Ministros. (2019). *Internet sano.* Recuperado de http://seguridadinformatica.sgp.gob.ar/paginas.dhtml?pagina=52

Leiva, E. A. (2015). Estrategias Nacionales de Ciberseguridad: Estudio comparativo basado en Enfoque Top-Down desde una visión global a una visión local. *Revista Latinoamericana de Ingeniería de Software, 3*(4), 161-176.

Lex Magiste. (2019). *Portaria Normativa No.3.389, de 21 de dezembro de 2012.* Recuperado de http://www.lex.com.br/legis_24068327_PORTARIA_NORMATIVA_N_3389_DE_21_DE_DEZEMBRO_DE_2012.aspx

Ley No.19.607-18. (2018) *Apruébese el acuerdo entre el Gobierno de la República Oriental del Uruguay y el Gobierno de la Federación de Rusia sobre la Cooperación en Materia de Defensa, suscrito en la cuidad de Moscú, Federación de Rusia, el 16 de febrero 2017.* Cámara de Representantes, Montevideo, Uruguay. Recuperado de https://medios.presidencia.gub.uy/legal/2018/leyes/04/mrree_1479.pdf

Ley No.20.478-10. (2010). *Sobre Recuperación y Continuidad en Condiciones Críticas y de Emergencia del Sistema Público de Telecomunicaciones.* Biblioteca del Congreso Nacional de Chile. Recuperado de https://www.leychile.cl/Navegar?idNorma=1020622&buscar=20478

Ministerio de Justicia y Derechos Humanos. (2019). *Atención a las víctimas.* Recuperado de http://www.jus.gob.ar/atencion-al-ciudadano/atencion-a-las-victimas/equipo-nin@s.aspx

Ministerio de Modernización de la República de Argentina y Ministerio de Energía, Turismo y Agenda Digital del Reino de España. (2017). *Memorando de Entendimiento sobre Cooperación en Materia de Ciberseguridad entre el Ministerio de Modernización de la República Argentina y el Ministerio de Energía, Turismo y Agenda Digital del Reino de España.* Recuperado de http://www.cecra.com.ar/binarydata/file/convenios/bilpai11182.pdf

Ministerio de Modernización. (2019). *¿Qué Hacemos?* Recuperado de https://www.argentina.gob.ar/que-hacemos

Ministerio de Tecnologías de la Información y Comunicación. (s.f.). *Institucional.* Recuperado de https://www.cert.gov.py/index.php/certpy

Ministerio del Interior y Seguridad Pública. (2019). *Decretos*. Recuperado de https://www.csirt.gob.cl/decretos/

Ministerio del Interior y Seguridad Pública. (2019). *Funciones.* Recuperado de https://www.csirt.gob.cl/funciones/

Ministerio Público (2019). *Delitos informáticos*. Recuperado de https://www.ministeriopublico.gov.py/delitos-informaticos-i242

Moreno, G. (2018). ¿Cuántos usuarios de internet hay en América Latina? *Statista.* Recuperado de https://es.statista.com/grafico/13903/cuantos-usuarios-de-internet-hay-en-america-latina/

Moreno, J. C., & Gil, M. M. L. (2017). Crisis y ciberespacio: Hacia un modelo integral de respuesta en el Sistema de Seguridad Nacional. *Cuadernos de Estrategia, 185,* 65-96.

Natalevich, M. (2017). Uruguay sufrió 15 ciberataques de alta severidad durante 2016. *El Observador.* Recuperado de https://www.elobservador.com.uy/nota/uruguay-sufrio-15-ciberataques-de-alta-severidad-durante-2016-2017123500

Núñez, C. (2019). *Estrategias Nacionales de Ciberseguridad en el Cono Sur. Análisis a partir de los indicadores de la Organización para la Cooperación y el Desarrollo Económico.* (Tesis inédita de maestría). Facultad de Humanidades, Universidad de Santiago de Chile, Chile.

OEA & Symantec. (2014). *Tendencias de seguridad cibernética en América Latina y el Caribe.* Recuperado de https://www.symantec.com/content/es/mx/enterprise/other_resources/b-cyber-security-trends-report-lamc.pdf

Organisation for Economic Cooperation and Development. (2012). Cybersecurity policy making at a turning point: Analysing

a new generation of national cybersecurity strategies for the internet economy. *OECD Publishing.*

Organización de Estados Americanos. (2015). Iniciativa de la Seguridad Cibernética de la OEA. *Foro Global sobre Experticia Cibernética.* Recuperado de https://www.sites.oas.org/cyber/Documents/2015%20Iniciativa%20de%20Seguridad%20Cibern%C3%A9tica%20de%20la%20OEA.PD

Organización de Estados Americanos. (2019). *Programa de ciberseguridad.* Recuperado de http://www.oas.org/es/sms/cicte/prog-ciberseguridad.asp

Pardo, D. (2013). Por qué Brasil está en el centro del escándalo de espionaje en EE. UU. *BBC Mundo.* Recuperado de https://www.bbc.com/mundo/noticias/2013/08/130822_tecnologia_brasil_snowden_eeuu_dp

Plan Ceibal. (2019). *Jóvenes a programar.* Recuperado de https://jovenesaprogramar.edu.uy/

Plan Ibirapitá. (2019). *El Plan.* Recuperado de https://ibirapita.org.uy/#el-plan

Policía de Investigaciones de Chile. (2019). *Cibercrimen.* Recuperado de http://www.pdichile.cl/instituci%C3%B3n/unidades/cibercrimen

Resolución No.580. (2011). Crea el Programa Nacional de Protección de Infraestructuras Críticas de Información y Ciberseguridad. *Información Legislativa.* Buenos Aires, Argentina. Recuperado de http://servicios.infoleg.gob.ar/infolegInternet/anexos/310000-314999/314171/norma.htm

Sánchez de Rojas, E. (2010). La ciberseguridad: Retos, riesgos y amenazas. *Revista Ejército*, *837,* 136-143.

Sancho, C. (2017). Ciberseguridad. Presentación del dossier/cybersecurity. Introduction to dossier. URVIO – *Revista Latinoamericana de Estudios de Seguridad, 20*, 8-15. doi: doi.org/10.17141/urvio.20.2017.2859

Secretaría Nacional de Tecnologías de la Información y Comunicación. (2017). *Plan Nacional de Ciberseguridad. Retos, roles y compromisos.* Recuperado de http://gestordocumental.senatics.gov.py/share/s/zkKW1CkKScSvapqlB7UhNg

Segura, R. (2018). Ciberdelitos íntimos. *Abc COLOR.* Recuperado de http://www.abc.com.py/edicion-impresa/suplementos/abc-revista/ciberdelitos-intimos-1755966.html

SID- Sistema de identidad digital (2019). Recuperado de https://www.argentina.gob.ar/sid-sistema-de-identidad-digital

Statista. (2019). *Volumen de pérdidas generadas por los delitos informáticos en determinados países en agosto de 2015 (en millones de USD).* Recuperado de https://es.statista.com/estadisticas/600983/ciberdelitos-indice-de-perdidas-en-determinados-paises-5/

Subsecretaría de Telecomunicaciones. (2018). *Gobiernos de Chile e Israel firman acuerdo de cooperación en el ámbito de ciberseguridad en las telecomunicaciones.* Recuperado de http://www.pdichile.cl/instituci%C3%B3n/unidades/cibercrimenhttps://www.subtel.gob.cl/gobiernos-de-chile-e-israel-firman-acuerdo-de-cooperacion-en-el-ambito-de-ciberseguridad-en-las-telecomunicaciones/

TeleGeography. (2019). *Submarine cable FrequentlyAsked-Questions.* Recuperado de https://www2.telegeography.com/submarine-cable-faqs-frequently-asked-questions?__hstc=196094579.1decb70f607f20f485981d351f-230cd6.1557275976667.1557275976667.1557275976667.1&__hssc=196094579.2.1557275976667&__hsfp=721576298

Timbó. (2019). *Trama interinstitucional multidisciplinaria de bibliografía online.* Recuperado de http://www.timbo.org.uy/

Van Bendegem, J. M. F. (2016). La quinta dimensión digital. bie3: *Boletín ieee, 4,* 834-859.

Viollier, P. (2017). *La participación en la elaboración de la Política Nacional de Ciberseguridad: Hacia un nuevo marco normativo en Chile.* Recuperado de https://www.derechosdigitales.org/wp-content/uploads/ciberseguridad.pdf