Capacidades estatales y Pandemia:
La Ciberseguridad en el Cono Sur entre el 2000 y el 2020[1]

Carla Gebetsberger
carla.gebetsberger@cari.org.ar
Secretaría Académica del Consejo Argentino para las Relaciones Internacionales (CARI).
María Paula Mareco
paula.mareco@gmail.com
Guillermo Spinoso
guillermoespinoso@gmail.com
Universidad de Buenos Aires
Sofía Vega Buono
sofiavega.buonovs@gmail.com
Universidad Nacional de Lanús

[1] El presente trabajo es parte de un proyecto de investigación producido en el marco del Grupo de Trabajo de Políticas Digitales y Ciberespacio del Consejo Argentino para las Relaciones Internacionales.

Resumen

El aumento de la digitalización, acompañado por una mayor cantidad, variedad y complejidad de ciberataques en los últimos años, ha generado en los Estados la necesidad de reforzar la estabilidad y seguridad en el ciberespacio. La pandemia cristalizó aún más sus vulnerabilidades. A través del relevamiento de las capacidades estatales en materia de ciberseguridad, producto de las Estrategias Nacionales de Seguridad Cibernética, del Cono Sur (Argentina, Brasil, Chile, Paraguay y Uruguay) en los últimos veinte años se busca comprender el estado de la seguridad informática actual frente al incremento de las ciber-amenazas durante la pandemia.

***Palabras claves**: Ciberseguridad, Cono Sur, Capacidades Estatales.*

Abstract

The increase of digitization, accompanied by a greater number, variety and complexity of cyberattacks over the last few years, has arisen the need for states to reinforce stability and security in cyberspace. Covid-19 pandemic further crystallized its vulnerabilities and inequalities. Through the survey of state capacities in cybersecurity in the Southern Cone (Argentina, Brazil, Chile, Paraguay and Uruguay) in the last twenty years, we seek to understand the current state of information security in the face of cyber-threats increase during the pandemic.

***Key Words**: Cyber Security, Southern Cone, State Capacities.*

I. Introducción.

En los últimos años se ha puesto en evidencia la necesidad de reforzar la estabilidad y la seguridad del ciberespacio. Este año se estima que son alrededor de 4,500 millones de personas las que tienen acceso a Internet a nivel mundial, al mismo tiempo que se acrecienta la cantidad, variedad y complejidad de ciberataques, tendencia profundizada por el COVID-19.

El trabajo aquí presente busca atender a este interrogante a través del relevamiento de las capacidades estatales en materia de ciberseguridad en el Cono Sur en los últimos veinte años (2000-2020). Para ello, en la sección II de este trabajo se delinea un marco teórico que cruza elementos del análisis de la gestión pública (Maltus, 1987; Bernazza, Comotto y Longo, 2015) y en materia de ciberseguridad (Alvaro Gomez Vieites, 2011; Hathaway, 2015; Leiva, 2015; Luiijf et. al, 2013) para conducir a un análisis de las Estrategias Nacionales de Seguridad Cibernética en las siguientes secciones.

Teniendo en cuenta que las estrategias y planes nacionales en ciberseguridad del Cono Sur han encontrado su fundamentación a partir del avance sostenido de la digitalización de sus sociedades y de su administración pública, por un lado, y del aumento de los ciberataques, por otro, se esbozan en la sección III las principales coordenadas de estas dos dimensiones, a partir de los datos oficiales suministrados por cada uno de los países. La sección IV aborda las Estrategias Nacionales de Seguridad Cibernética en cada uno de los países del Cono Sur, a partir de los micro indicadores delineados en el marco teórico. Finalmente, se buscará, en la sección V, revisar la respuesta de los países ante la pandemia y si en sus respuestas incluyeron o no modificaciones los indicadores analizados.

II. Marco teórico.

Entre las dificultades presentes a la hora de abordar la investigación sobre los diversos enfoques estatales en materia de ciberseguridad se encuentra la falta de definiciones del término por parte de los Estados, en primer lugar, y la falta de homogeneidad en las definiciones existentes, en segundo. Este fenómeno no es exclusivo de las naciones del Cono Sur sino que por el contrario es compartido por la mayoría de los Estados. Luiijf, Besseling, Spoelstra y de Graaf (2013) son algunos de los autores que indagan en la cuestión, para descubrir en su análisis de las estrategias de ciberseguridad nacional de diez Estados que no existe tal cosa como una definición ampliamente aceptada, sino que por el contrario cada Estado confecciona una definición de ciberseguridad funcional a sus intereses particulares, o en muchos casos jamás define el término con claridad[2]. En algunas definiciones se pone el foco en la seguridad de la información, mientras que en otras se toma a la ciberseguridad como una herramienta para enfrentar y contrarrestar las amenazas provenientes del ciberespacio. Pese a esta falta de consenso desde las estructuras estatales sobre la definición de ciberseguridad, a los términos del presente trabajo adscribimos a aquella formulada por Gomez Vieites, quien define seguridad informática (usada como sinónimo para "ciberseguridad") como:

> "*cualquier medida que impida la ejecución de operaciones no autorizadas sobre un sistema o red informática, cuyos efectos puedan conllevar daños sobre la información, comprometer su confidencialidad, autenticidad, o integridad, disminuir el rendimiento de los equipos o bloquear el acceso de usuarios autorizados al sistema (2011, p. 38)."*

Pese a que en América Latina y el Caribe los esfuerzos por lograr la estabilidad y la seguridad del ciberespacio están en una etapa temprana (Banco Interamericano de Desarrollo – BID- y Organización de los Estados Americanos- OEA-, 2020), se ha destacado que los países del Cono Sur (Argentina, Brasil, Chile, Paraguay y Uruguay) se posicionan "dentro de un rango medio, a nivel mundial, hacia el desarrollo de su ciberseguridad nacional" (ITU Publications, 2018) y su nivel de madurez en ciberseguridad es el más alto de América Latina y el Caribe.

En las últimas dos décadas, la región del Cono Sur comenzó a adoptar medidas tendientes a reafirmar el papel de las TIC en la gestión pública. En materia de ciberseguridad, los marcos regulatorios y desarrollo de capacidades nacionales encuentran sus más tempranos antecedentes a mediados y fines de la década de los noventa. A partir del cambio de siglo, el

[2] Los autores analizan las ENSC de Australia, Canadá, República Checa, Francia, Alemania, Japón, Holanda, Nueva Zelanda, Reino Unido y Estados Unidos. De estas diez naciones, sólo cinco hacen explícita su definición del término "ciberseguridad".

diseño de estrategias nacionales de ciberseguridad comenzó a desarrollarse más activamente en la región, y se aceleró significativamente en el transcurso la segunda mitad de la última década. Con los marcos regulatorios primarios establecidos, se presentó un período de ralentización en el desarrollo de capacidades. Sin embargo, en los últimos cinco años (2015-2020), la creación de estándares, organizaciones y tecnologías reflejaron una mayor preocupación en la materia.

¿Cómo ordenar, en clave regional, el diseño de capacidades estatales en ciberseguridad impulsadas en Argentina, Brasil, Chile, Paraguay y Uruguay? Se llevará adelante un relevamiento que busca ser representativo de los elementos constitutivos de las capacidades estatales, por lo cual, el mismo se concentrará en aquello que es definido por Carlos Matus (1987) como proyecto de gobierno que, junto a las capacidades estatales y la gobernabilidad del sistema, es el primer elemento de la tríada denominada triángulo de gobierno. El proyecto de gobierno queda así definido por Matus como "*el contenido propositivo de los proyectos de acción que un actor se propone realizar para alcanzar sus objetivos"* (1987: 74). En materia de ciberseguridad, se trata de la primera y más importante área que indica la preparación cibernética de un país (Hathaway, 2015), 2015: 6): refiere a la articulación y publicación de una Estrategia Nacional de Seguridad Cibernética que alinea la visión del país con sus imperativos de seguridad nacional. Más precisamente, puede ser definida como "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).

La ENSC consolida "una serie de objetivos nacionales y prioridades proporcionando 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).

Se buscará aquí prestar especial atención al proyecto institucional de los proyectos de gobierno en materia de ciberseguridad, las ENSC, en Cono Sur entre el 2000 - momento en el que comenzaron a desarrollarse más activamente, como se mencionó con anterioridad- y el 2020. Se entenderá por proyecto institucional aquí a "una voluntad puesta en acto capaz de configurar las rutinas, los procesos, las actividades y los resultados a obtener, debemos relevar su presencia en la vida de la institución" (Bernazza, Comotto y Longo, 2015). Conocer la real implicancia institucional del proyecto será preciso, en una investigación futura para evaluar la correspondencia con los resultados institucionales obtenidos. En la siguiente tabla se ordenan los datos a relevar y sus micro indicadores:

Tabla 1. Micro Indicadores del Proyecto Institucional

Dato a relevar	**Fuentes e instrumentos de relevamiento**
Plan integral de la Estrategia Nacional de Seguridad Cibernética	-Declaraciones o documentos que refieran a un plan de acción integral y/o sectorial. -Alusión a un plan de tipo integral en el plan sectorial de la institución. -Alusión al plan integral y/o sectorial en programas y proyectos institucionales. -Aprobación del plan integral y/o sectorial, o de alguno de sus componentes, a través de leyes o actos administrativos del organismo. -Alusión al plan integral y/o sectorial en piezas comunicativas gráficas o audiovisuales diseñadas por la institución. -Alusión al plan integral/sectorial en piezas comunicativas o normas emanadas del poder Ejecutivo u otros organismos.
Bienes y servicios brindados en relación con las competencias institucionales y el plan expresado.	Relevamiento de bienes o servicios efectivamente brindados. Relación de estos bienes y servicios finales con las competencias institucionales y los objetivos del plan previsto. Cantidad, calidad y alcance o cobertura territorial.

Fuente**:** Elaboración propia en base a la Guía de indicadores e instrumentos para la medición de capacidades estatales (Bernazza, Comotto y Longo, 2015).

III. Los fundamentos de las ENSC: la digitalización y los ciberataques.

Debido a que las ENSC del Cono Sur han encontrado su fundamentación a partir del avance sostenido de la digitalización, por un lado, y del aumento de los ciberataques, por otro, se esbozan las principales coordenadas de estas dos dimensiones, a partir de los datos oficiales suministrados por cada uno de los países.

III. i. Digitalización

Es innegable el asombroso desarrollo de las tecnologías de comunicación e información (TIC) durante el Siglo XXI, el cual atestigua un sostenido incremento global de la digitalización en los últimos veinte años. Esta afirmación es válida también para la región de Latinoamérica y el Caribe. De acuerdo con las mediciones del Observatorio de TIC de la Corporación Andina de Fomento (CAF) (2017), el ecosistema digital de la región ha crecido al menos un 106.87% en diez años: en 2004 había alcanzado un índice de 21.98 (en una escala de 0 a 100), mientras que para el 2015 su índice de desarrollo era del 45.47, con una tasa de crecimiento del 6.83% anual. Algunas de las áreas que exhibieron crecimientos más significativos fueron la digitalización de hogares, las mejoras en la conectividad y en los niveles de competencia.

Este desarrollo no ha sido homogéneo en toda América Latina y el Caribe. Para el año 2015, los índices de los países de la región exhibían desigualdades significativas: mientras que ocho naciones contaba con un índice mayor a 50, lo cual se corresponde con un ecosistema avanzado (Chile 60, Barbados 57, Colombia 55, Uruguay 53, Trinidad y Tobago 52, Argentina 51, Brasil 51, Costa Rica 50), otras cinco naciones se encontraban por debajo de 40 en el índice CAF de desarrollo del ecosistema digital, lo que corresponde a un ecosistema limitado (República Dominicana 39, Perú 38, Paraguay 35, Jamaica 35 y Bolivia 30).

Las cifras de este año del Observatorio CAF del Ecosistema Digital (2020) de América Latina y el Caribe en digitalización, muestran que la región se encuentra en una situación de desarrollo intermedio. Su índice es de 49.92, en una escala de 0 a 100, donde otras regiones como África y Asia Pacífico se encuentran menos favorecidas, con índices de 35.05 y 49.16 correspondientemente, pero donde otras como Europa Occidental, con un índice de 71.06 y América del Norte, cuyo índice es de 80.85 dejan rezagada a la región (Corporación Andina de Fomento - Banco de Desarrollo de América Latina, 2020).

Las últimas estadísticas disponibles señalan una penetración de Internet en los hogares latinoamericanos del 68.66% en 2018, mientras que estimativos proyectan esta penetración en el

78.78% para el año 2020[3]. A modo de comparación, el promedio ponderado proyectado en el mismo año para los países de la OCDE es del 88.33% de penetración de Internet en los hogares. Las cifras no obstante ocultan una realidad en nuestra región y es que se halla una gran dicotomía entre los sectores urbanos y rurales al interior de cada Estado. Por nombrar algunos ejemplos, mientras que las áreas urbanas de Bolivia mostraban en 2014 un nivel de adopción del 20.6%, esta cifra descendía al 1.7% en las áreas rurales; para Brasil en 2017 el nivel de adopción era del 65.1% en áreas urbanas pero del 33.6% en áreas rurales, entre otros casos similares (ITU World Telecommunication/ICT Indicators database, 2020).

Dentro de América Latina, el Cono Sur es el área con mayor penetración y uso de Internet (Internet World Stats, 2018). En el 2018, los porcentajes de la población de Argentina, Brasil, Chile, Paraguay y Uruguay que utilizaban esta herramienta tecnológica se encontraban entre los más altos de toda América Latina[4]. Esto se explica en parte por el relativamente bajo costo del acceso a las telecomunicaciones en forma de canastas de datos móviles en esos países, el cual representa entre el 1% y 1.8% de la renta nacional per cápita (RNB p.c.) en los casos de Argentina, Brasil, Chile y Uruguay.[5] A modo de referencia, el promedio de toda América Latina para el costo de canastas de datos móviles es el 3.02% de la RNB p.c.

Debido a la pandemia de SARS-CoV-2 sufrida durante el 2020, el acceso difundido a las tecnologías de comunicación e información se ha vuelto una estrategia clave desarrollada por los Estados, el sector privado y los individuos para continuar desarrollando sus actividades en un contexto que ha impuesto los aislamientos, cuarentenas preventivas y trabajos a distancia como medidas de seguridad. Frente a tales desafíos, el gran interrogante para muchos expertos fue cómo enfrentaría la región estos dilemas y si saldría triunfante en sus estrategias de adaptación a un nuevo contexto tan complejo. De manera similar a todo el globo, en América Latina se incrementó el tráfico en las redes de Internet. Esto puede verse en la disminución de la velocidad de la banda ancha fija por demanda incrementada, como es el caso de Chile que exhibió un descenso de más de 3 Mbps (velocidad en la que viajan los datos desde la Web a la PC o el celular por segundo) entre el mes de febrero de 2020 y la tercera semana de Marzo de 2020 (en que comenzaron a regir las medidas de cuarentena en el país).

Otro indicador del tráfico aumentado en la región es el incremento de la latencia tanto de la banda ancha fija como móvil. Numerosos países mostraron incrementos en este indicador al comparar la primera semana del mes de marzo de 2020 con la última del mismo mes (Brasil

[3] Los datos del 2020 han sido extrapolados en base a la tasa de crecimiento del último año con información provista por la UIT. Fuente: Unión Internacional de Telecomunicaciones; análisis Telecom Advisory Services.

[4] Argentina 93.10%, Brasil 70.70%, Chile 77.50%, Paraguay 89.60% y Uruguay 88.20% (Internet World Stats, 2018)

[5] Chile menor al 1% de la RNB p.c., Argentina 1.3% de la RNB p.c., Uruguay 1.6% de la RNB p.c., Brasil 1.8% de su RNB p.c., Paraguay, 4.4% de la RNB p.c. (ITU, 2019).

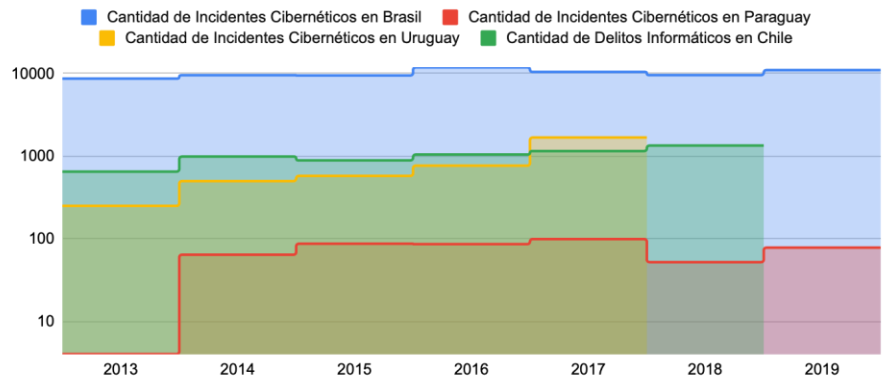
de 17 a 19, Chile de 21 a 25, Ecuador de 17 a 19, México de 27 a 29). Estos aumentos representan una erosión de la calidad del servicio.

Simultáneamente a estos picos y alteraciones puntuales, los cuales plantean dificultades coyunturales para los usuarios pero también para las administraciones públicas y sector privado al trasladar sus operaciones diarias a la dimensión digital, se esbozan para la región limitaciones estatales más profundas ante los ciberataques.

III. ii. Ciberataques, avances o anuncios a nivel mundial y regional

En el Cono Sur, los principales agentes oficiales que recopilan los incidentes cibernéticos a nivel nacional son los Centros y Equipos de Respuesta ante Incidentes de Seguridad Informática (CERTs). Se trata de la única fuente de datos oficiales en cada uno de estos países. Desde el año 2013, Brasil, Chile, Paraguay y Uruguay han publicado información sobre los incidentes cibernéticos en sus países a través de sus Centros y Equipos de Respuesta ante Incidentes de Seguridad Informática. A partir de la información suministrada por estos países, en el Gráfico 1 se reúne la cantidad de ataques e incidentes cibernéticos por año en cada país. Es importante destacar que los periodos de tiempo de relevamiento difieren de país a país.

Gráfico 1.



Ciberataques en Brasil, Chile, Paraguay, Uruguay

Fuente: Elaboración propia a partir de datos publicados por CERT-BR (Brasil); CLCERT (2016-2018); Ministerio Público (ULDDECO, 2010-2015); Policía De Investigación y el Ministerio Público (Unidad Especializada en Lavado de dinero, Delitos Económicos y Crimen Organizado) (Chile); CERT-PY (Paraguay); y, CERT-UY (Uruguay).

Tal como es reflejado en el Gráfico 1, Brasil es el caso con mayor cantidad de incidentes y ataques cibernéticos, seguido por Chile, Uruguay y Paraguay. Durante el año 2017, los ciberataques aumentan en Uruguay, sobrepasando el número de Paraguay por vez primera

desde el año 2012, momento en que sus Centros de Respuesta empiezan a publicar la información disponible.

Pese a que el aumento de ciberataques es entendido como elemento fundante de las ENSC, a partir de los datos oficiales disponibles no se percibe una relación clara con los momentos de creación y actualización de las estrategias. Cabría, no obstante, cuestionar la robustez de los datos publicados ya que la desagregación detallada y completa de los delitos y ataques cibernéticos es una tarea aún pendiente debido a la falta de claridad conceptual, la carencia de registros sólidos y a la baja cantidad de denuncias (Núñez, 2019). De todas maneras, aún escapando a una relación empíricamente comprobable en los hechos cibernéticos, no deja de ser destacable que tanto la formulación como la actualización de todas las ENSC en el Cono Sur se han fundado frente a un diagnóstico de ataques cibernéticos en aumento.

IV. El Proyecto Institucional de gobierno: las Estrategias Nacionales de Seguridad Cibernética (ENSC) en el Cono Sur (2000-2020).

En la última década, a raíz de la aceleración de la digitalización y un aumento de ciberataques, los distintos gobiernos del Cono Sur han comenzado a elaborar y/o actualizar sus ENSC con el objetivo de modernizar los resguardos nacionales en asuntos cibernéticos y hacer frente a las amenazas emergentes provistas por las nuevas tecnologías.

País	**Año**	**Nombre del Proyecto de Gobierno**
Argentina	2015	Estrategia Nacional de Ciberseguridad
	2019	Estrategia Nacional de Ciberseguridad
Brasil	2015	Estrategia Nacional de Seguridad de las Comunicaciones de Información y Seguridad Cibernética de la Administración Pública Federal
	2020	Estrategia Nacional de Ciberseguridad (E-Ciber)
Chile	2015	Agenda Digital 2020
	2017	Política Nacional de Ciberseguridad
Paraguay	2017	Plan Nacional de Ciberseguridad de Paraguay
Uruguay	2005	Agenda Uruguay Digital
	2009	Política de Seguridad de la Información para Organismos de la Administración Pública
	2016	Marco de Ciberseguridad
	2019	Agenda Uruguay Digital 2020

Las páginas que siguen resumen la formulación de las ENSC en cada uno de los países del Cono Sur y avanzan sobre los principales productos del proyecto institucional que fueron generados dentro de dicho marco:

IV.i. Argentina

Argentina fue uno de los primeros países de la región en desarrollar un Equipo de Respuesta ante Incidentes de Seguridad Cibernética (Banco Interamericano de Desarrollo y Organización de los Estados Americanos, 2016). En el año 1999, se creó el reglamento de Operación del ArCERT, cuya función era adecuar las políticas de seguridad y centralizar los reportes de incidentes, y desde abril de 2004 formó parte del FIRST (Forum de Respuesta a Incidentes y Equipos de Seguridad Informática). En el año 2011 pasó a formar parte del Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad (ICIC) (Banco Interamericano de Desarrollo y Organización de los Estados Americanos, 2016) de la Oficina Nacional de Tecnología de Información (ONTI), creada ese mismo año.

En 2013 se creó el ***Grupo de Trabajo "ICIC - CERT***", responsable de administrar toda la información sobre reportes de incidentes de seguridad en el Sector Público Nacional que hubieran adherido al Programa Nacional antes mencionado y en 2016 se creó el BA-CSIRT, un centro de expertos en ciberseguridad en Ciudad de Buenos Aires. BA-CSIRT tiene firmados convenios con otros centros de ciberseguridad del mundo, y en particular es el CSIRT argentino que se vincula con la OEA. Desde noviembre del 2017, el país también suscribe al Convenio de Budapest sobre Delito Cibernético, aprobado en la Ley 27.411 y participa en el "Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal" del Consejo de Europa, siendo uno de los pocos países de América.

El desarrollo de la ***Estrategia Nacional de Ciberseguridad*** (ENCS), aprobada en 2019 según la resolución 829 en conjunto con la Unidad Ejecutora, se encuentra a cargo del Comité de Ciberseguridad. Argentina también creó el Programa Nacional de Infraestructura de Información Crítica y Ciberseguridad (ICIC-CERT) que, a pesar de no ser miembro de CSIRT Américas, colabora con el sector privado. Además, cuenta con la Dirección Nacional de Ciberseguridad, dentro de la Jefatura de Gabinete de Ministros, con la Subsecretaría de Ciberdefensa, perteneciente al Ministerio de Defensa y de la Dirección de Cibercrimen en el Ministerio de Seguridad, y con la Unidad Fiscal Especializada en Ciberdelincuencia (UFECI) y fiscalías especializadas en cibercrimen a nivel jurisdiccional (de la Ciudad Autónoma de Buenos Aires). Por último, es necesario incorporar el desarrollo del Plan Federal de Prevención de Delitos Tecnológicos y Ciberdelitos para los años 2019-2023 dentro del cual se creará el Centro de Coordinación de Combate al Ciberdelito.

Argentina fue de los primeros países del continente americano en crear un marco regulatorio para la protección de datos personales, que actualiza y refuerza. A fin de enmarcar distintas figuras delictivas del mundo digital, buscó avanzar sobre modificaciones en la legislación existente. En el año 2000 promovió la ***Ley de Protección de Datos Personales*** (25.326), con el objetivo de definir principios generales relativos a la protección de datos. A su

vez, la modificación de la Ley de Propiedad Intelectual (Ley 11.723) actúa sobre las obras científicas, literarias y artísticas. Además, comprende los "escritos de toda naturaleza y extensión, entre ellos los programas de computación fuente y objeto". Por otra parte, la Ley de Delitos Informáticos (Ley 26.388) tiene como objetivo regular las nuevas tecnologías como medios de comisión de delitos previstos en el Código. Por último, la Ley de Grooming (Ley 26.904), sancionada en noviembre de 2013, pena un delito que continúa en alarmante aumento.

IV. ii.Brasil

En el año 2015, durante la presidencia de Dilma Rousseff (2011- 2016), fue publicada la ***Estrategia Nacional de Seguridad de las Comunicaciones de Información y Seguridad Cibernética de la Administración Pública Federal 2015 – 2018***, con el objetivo de "fortalecer a política e o planejamento de segurança da informação e comunicações e de segurança cibernética na Administração Pública Federal, visando assegurar e defender os interesses do Estado e da sociedade para a preservação da soberania nacional." (Departamento de Segurança da Informação e Comunicações, 2015, p.37).

Brasil formalizó la Estrategia Nacional de Ciberseguridad (E-Ciber), aprobada en febrero de 2020, y fue el primer gran intento de desarrollar, de manera coordinada, una mirada de la ciberseguridad de manera abarcativa. Aún no ha adherido a la Convención de Budapest sobre Delito Cibernético, a pesar de estar atravesando el proceso de adaptación legal para unirse desde mediados de 2019, fecha desde la cual tiene permitido asistir como Estado Observador a las reuniones sobre la Convención y sus protocolos[6].

Con respecto a sus capacidades, desde 2005 cuenta con el NIC.br (*Network Information Center*), una de las organizaciones más importantes en la coordinación de diferentes aspectos técnicos de la gobernanza de internet, abarcando junto con CERT.BR (creado en 1997) y Registro.br la responsabilidad de registrar y mantener nombres de dominios ".br", y la definición e implementación de estándares de seguridad de distribución de direcciones de IP.

La arquitectura de organismos de ciberseguridad tiene su centro en el Gabinete de Seguridad Institucional (GSI), que se ocupa de los aspectos civiles y del asesoramiento asuntos militares y la ciberdefensa. El GSI subordina muchos organismos destinados a la ciberseguridad, como el Departamento de Seguridad de Comunicación e Información (DSIC), la Secretaría de Asuntos Estratégicos (SAE) y la Cámara de Asuntos Estratégicos y Defensa Nacional del Consejo de Gobierno (CREDEN), instituciones fundamentales en la construcción de ciberseguridad en Brasil. El desarrollo institucional surgió en gran parte de la doctrina

[6] Ministerio de Relaciones Exteriores de Brasil http://www.itamaraty.gov.br/es/notas-a-la-prensa/21150-proceso-de-adhesion-a-la-convencion-de-budapest-nota-conjunta-del-ministerio-de-relaciones-exteriores-y-el-ministerio-de-justicia-y-seguridad-publica

establecida por el Centro de Defensa Cibernética (CDCiber) de 2012, como el órgano responsable de integrar y coordinar actividades de ciberdefensa. Otros ministerios, como el de Ciencia y Tecnología, incluyeron a la ciberseguridad (aunque sólo tangencialmente) en la Estrategia de Transformación Digital (2018), buscando un enfoque holístico, alineado con planes de acción para diferentes partes de los gobiernos.

La legislación brasileña se basa en disposiciones de la Constitución Federal, en el Código Penal de Brasil, en el Marco de Derechos Civiles de Brasil, en el Código de Protección al Consumidor y en la Ley General de Protección de Datos para garantizar la protección de la privacidad en Internet. La ***Ley de Delitos Cibernéticos***, también conocida como la "Ley Carolina Dieckmann", y el ***Marco Civil de Internet*** de Brasil se consideran los instrumentos legislativos vigentes más pertinentes y sustantivos y tienen por objeto manejar formalmente los delitos cibernéticos y otorgar facultades procesales al manejar pruebas electrónicas.

El Marco Civil y la Ley de Protección de Datos (aprobada en 2018 y en vigor desde este año), buscan integrar la seguridad de la información con un enfoque más amplio que incluya la privacidad y la administración de datos de manera segura. En las tareas de ciberseguridad a nivel nacional también participan actores de inteligencia (ABIN), la Policía Federal (bajo la supervisión del Ministerio de Justicia), empresas privadas y CSIRTS privados. En los últimos tres años ha habido un fuerte impulso en la creación de marcos legales, iniciativas y estándares de concientización, organizaciones y tecnologías.

Previo a la pandemia Brasil era el país con mayor cantidad de incidentes cibernéticos por año en comparación a Chile, Paraguay y Uruguay. Cabe destacar que en la última década se produjo en Brasil un incremento de ataques durante los "mega eventos" entre 2012 y 2016, como los JJOO, la Copa Mundial de Fútbol y Río+20, a partir de los cuales la ciberseguridad se volvió un tema más importante a nivel nacional.

IV. iii.Chile

La complejidad y cantidad de los delitos informáticos que han aquejado a Chile a partir de 2015, han despertado la necesidad de mayor recurso humano y tecnológico adecuado para su tratamiento. En este sentido, el gobierno de Michelle Bachellet, mediante el decreto Nº 533/15, estableció la creación del Comité Interministerial de Ciberseguridad (CICS)[7]. La misión principal del mismo consistía en desarrollar e implementar una estrategia de ciberseguridad robusta, sintetizada posteriormente en la Política Nacional de Ciberseguridad (PNCS) 2017-2020. Fijando cinco ejes y áreas estratégicas de trabajo -infraestructura, legislación, difusión y cultura de la ciberseguridad, cooperación internacional, y desarrollo de la industria-, la PNCS

[7] El Comité Interministerial se encuentra compuesto por la Subsecretaría del Interior, de Defensa, de Relaciones Exteriores, de Telecomunicaciones, de Justicia, de Economía y la Agencia Nacional de Inteligencia.

consignó la coordinación estratégica de los distintos organismos y entidades institucionales en materia de ciberseguridad, unificando esfuerzos, roles y funciones, y el establecimiento de prácticas y criterios técnicos comunes, con el objetivo de mejorar la eficiencia y eficacia de la seguridad cibernética. Considerando imprescindible contar con una estructura de prevención, monitoreo y gestión a nivel nacional, Chile cuenta con un ***Equipo de Respuestas ante Incidentes de Seguridad Informática*** nacional (CSIRT de Gobierno), el cual recopila y sistematiza información proveniente de otros CSIRT (nacionales y extranjeros), promoviendo la coordinación de acciones entre CSIRT sectoriales, y consolidando la autoridad suficiente para coordinar la respuesta técnica frente a incidentes que comprometan la seguridad del país. Bajo la órbita del Ministerio del Interior y Seguridad Pública, su misión, por tanto, es reducir los riesgos en ciberseguridad en las redes de gobierno. En concordancia, el Ministerio de Relaciones Exteriores, a través de ***la Dirección de Seguridad Internacional y Humana*** (DISIN), identifica, coordina y promueve la posición de Chile en la comunidad internacional en lo relacionado a la ciberseguridad, y se encarga de promover las relaciones bilaterales, fomentando la cooperación internacional bajo múltiples modalidades como la asistencia desde o hacia Chile, el intercambio de información y experiencias, y la implementación y profundización de mecanismos de diálogo político.

Como parte de las políticas complementarias en materia digital que plantea la PNCs se encuentra la ***Agenda Digital 2020***, que consiste en "una hoja de ruta que define los próximos pasos para concretar una política de desarrollo inclusivo y sostenible a través de las Tecnologías de la Información y la Comunicación (TIC)"[8]. El gobierno digital es uno de los ejes centrales de tal proyecto, junto con los derechos para el desarrollo digital, la conectividad digital, la economía digital y las competencias digitales. No obstante, el desarrollo tecnológico y la digitalización de los procesos han superado la velocidad de la actualización de la jurisprudencia en materia de ciberseguridad. La PNCS observa un conjunto de normas legales y reglamentarias sobre la ciberseguridad que resulta necesario revisar y actualizar conforme a las directrices que plantea esta política y a los compromisos internacionales de Chile. Es valioso aclarar que en el año 2017, Chile adhirió al Convenio de Budapest. Así, establece proyectos de ley que incluyen la nueva ley de Delitos Informáticos (N° 19.223); ley Marco de Ciberseguridad; ley de Infraestructura Crítica para la Ciberseguridad; y la ley de Protección de Datos.

IV. iv.Paraguay

Desde el año 2014, tras la solicitud del Gobierno de Paraguay para formar parte del Convenio de Budapest sobre Delito Cibernético, se inició la elaboración de un ***Plan Nacional***

[8] Sistema de información de tendencias educativas de América Latina (2018) https://www.siteal.iiep.unesco.org/sites/default/files/sit_accion_files/siteal_chile_5034.pdf

de Ciberseguridad a través de la Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs), y en coordinación con el Ministerio de Relaciones Exteriores (MRE). Fue finalmente aprobado en 2017 por el ***decreto 7052/17***, por medio del cual quedó integrada su Comisión Nacional de Ciberseguridad con representantes de distintas instituciones públicas, teniendo por objetivo adoptar medidas de seguridad cibernética que garanticen y promuevan el uso seguro y confiable de las TIC, así como el progreso y la innovación en el país. Sus ejes de acción se constituyeron a través de: sensibilización y cultura, investigación, desarrollo e innovación, protección de infraestructura crítica, capacidad de respuesta a incidentes cibernéticos, investigación y capacidad de enjuiciamiento cibernético, administración pública, y sistema nacional de seguridad cibernética. Este plan complementa y fortalece otras iniciativas que estaban ya siendo desarrolladas por parte del Estado como los proyectos de Gobierno Electrónico, las TIC en la educación e inclusión digital, despliegue de fibra óptica, firma digital, comercio electrónico, del ***Centro de Respuesta ante Incidentes Cibernéticos*** (CERT-PY), de la Unidad Especializada de Delitos Informáticos del Ministerio Público y de la División Especializada contra Delitos informáticos de la Policía Nacional, entre otros.

Actualmente, los incidentes informáticos son gestionados por el CERT-PY, miembro del CSIRT de las Américas, bajo la Dirección General de Políticas y Desarrollo de TIC de la SENATICs (Decreto N°11.624/2013). Se trata del organismo coordinador de incidentes cibernéticos que afectan al ecosistema digital de Paraguay (Informe CERT-PY, 2019). El CERT-PY brinda un servicio permanente de gestión de incidentes cibernéticos, disponible para cualquier persona u organización sin ningún costo. Cualquier ciudadano, empresa, institución pública u organización extranjera puede reportar un incidente cibernético que afecte a un sistema de información del ecosistema digital nacional, propio o de terceros.

En octubre de 2018 se creó, además, el Ministerio de Tecnologías de la Información y Comunicaciones (MITIC), uno de cuyos ejes estratégicos es la Ciberseguridad y Protección de la Información. A través de la Dirección General de Ciberseguridad y Protección de la Información, el MITIC cuenta hoy en día con los siguientes roles y atribuciones, establecidos en la Ley N° 6207/2018, que instituyó su creación:

- Construir un ecosistema digital seguro, confiable y resiliente, que incluya a los sectores público y privado, así como a la academia y la ciudadanía.
- Establecer políticas de protección de la información personal y gubernamental.
- Velar por la protección de sistemas, redes, procesos e información de los organismos y entidades del Estado.
- Idear planes y estrategias de ciberseguridad a nivel nacional.

- Ejercer la autoridad en ciberseguridad, prevención, gestión y control de incidentes cibernéticos.
- Definir y proteger la infraestructura tecnológica crítica.

IV. iv.Uruguay

Uno de los gobiernos latinoamericanos pioneros en la implementación de una agenda de políticas digitales es el uruguayo. Desde principios del 2000, la República Oriental del Uruguay lleva adelante la Agenda Uruguay Digital con el objetivo de avanzar "en la transformación digital de forma inclusiva y sustentable" (Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento, 2019) Desde el año 2009 y por medio del decreto N°451/009, el Uruguay cuenta con una política específica referida a ciberseguridad. En ese decreto se sientan las bases de esta política ya que en él se definen los conceptos de evento e incidente de seguridad informática, además de crearse el CERT-UY. Ese mismo año y mediante el decreto N°452/009 se formaliza la Política de Seguridad de la Información para Organismos de la Administración Pública, la cual rige para todos las dependencias estatales de Uruguay. Este texto busca promocionar la aplicación de un sistema de gestión de seguridad de la información para el Estado uruguayo. Desde agosto del 2016 el país también cuenta con un Marco de Ciberseguridad, el cual se encuentra en utilización y es periódicamente actualizado con el objetivo de preservar su calidad y vigencia.

Todas estas medidas, marcos regulatorios y organismos se enmarcan dentro de la Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento (AGESIC). Fundada en 2005 por medio de la ley N° 17.930, la agencia nuclea la implementación de las políticas digitales uruguayas, desde aquellas dirigidas a la población civil, como los Planes Ceibal e Ibirapitá, como también las referentes a los sistemas de gestión de seguridad de la información estatal. Únicamente se halla fuera de la esfera de competencia de la AGESIC y relacionado con el mundo digital el Departamento de Delitos Informáticos. Esta dependencia de la Dirección General de Lucha contra el Crimen Organizado e Interpol, por tanto, parte de la Policía Nacional, fue formada en 2019 mediante el Decreto N°84/019. Centra su accionar en la detección de delitos que pueden catalogarse como digitales por usar tecnologías de la informática como medio para el hecho, es por esto que no se puede afirmar que esté enteramente dedicado a cuestiones de ciberseguridad. Algunos de los casos que tratan sí tienen vínculo con la seguridad informática pero otros se tratan de delitos convencionales que utilizan las tecnologías de la información y el conocimiento únicamente como medio para su accionar. Es el caso de los delitos de fraude, producción, distribución y/o consumo de pornografía infantil, entre otros.

Pese al cambio de signo político ocurrido en el país en Marzo de 2020, la nueva administración en principio ha decidido no sólo continuar esta línea de política pública sino profundizarla e incentivarla. Recientemente en su discurso dirigiéndose a la Asamblea General de las Naciones Unidas, el flamante presidente uruguayo Luis Lacalle Pou dedicó unas palabras para expresar el apoyo de la nación al mapa de ruta sobre cooperación digital presentado por el Secretario General. Asimismo, destacó la importancia de superar la brecha digital y de conectividad debido al papel fundamental de las nuevas tecnologías para contribuir al cumplimiento de los Objetivos de Desarrollo Sostenible (ODS). Finalmente, el mandatario hizo hincapié en la centralidad de profundizar el desarrollo de la ciberseguridad, propugnando por una solución colaborativa entre actores estatales, el sector privado y la sociedad civil (Lacalle Pou, 2020).

V. El Cono Sur en pandemia.

El 23 de enero de 2020, el anuncio del encierro de la ciudad de Wuhan (11,8 millones de habitantes) en la provincia de Hubei (China) se inauguraron como hitos de una pandemia que trajo consigo una amplificación de dos tendencias: la profundización de la digitalización y el aumento de los ciberataques. ¿Cómo impactaron estas variables en las ENSC de los Estados de Cono Sur?

V.i.Argentina

El gobierno argentino, que asumió a finales de 2019, anunció ciertos cambios de lineamientos en relación al gobierno anterior y a tiempos previos de la pandemia. Un ejemplo de esto es el objetivo de pasar de una estrategia Nacional de Ciberseguridad a una Estrategia Federal de Ciberseguridad para acortar la brecha entre grandes centros urbanos y pequeños pueblos en trabajo conjunto con las provincias[9]. Además Gustavo Sain, director nacional de Ciberseguridad, sostuvo en julio que dado que "hay una preeminencia del sector privado y el sector público interviene a través de la administración de justicia cuando se comete un delito"[10], trabajará en conjunto con empresas privadas en la discusión sobre estrategias de seguridad que resulten preventivas del delito digital para defender los derechos de los ciudadanos.

La necesidad de aunar fuerzas responde a que, según la Asociación Argentina de Lucha Contra el Cibercrimen (AALCC), desde la implementación del Aislamiento Social Preventivo y Obligatorio, los delitos de extorsión online aumentaron un 20,42%, el phishing un 16,52%, y el fraude un 14,89%, en línea con lo acontecido en todo América Latina. A estos números hay que sumarle una serie de acontecimientos que tuvieron gran repercusión en la esfera pública y a nivel internacional: los grandes ciberataques.

Entre los que más destacan, se encuentran los secuestros de información a través de ransomware de la empresa prestadora de Internet Telecom y de la Dirección Nacional de Migraciones. Telecom Argentina, uno de los principales proveedores de servicios de Internet (ISP) fue víctima de un ransomware a fines de julio, según un informe local. El rescate exigido para desbloquear los archivos encriptados fue de $7,5 millones de dólares en criptomonedas Monero. Sin embargo, la compañía afirmó haber restaurado el acceso a sus sistemas rápidamente y no tuvo impacto significativo en los servicios proporcionados.

---

[9] Argentina.gob.ar, 16 de julio de 2020.
[10] Télam, 5 de julio de 2020.

Por otra parte, a finales de agosto, ciberdelincuentes atacaron a la Dirección Nacional de Migraciones (más específicamente a la Dirección de Asuntos Migratorios, área responsable de realizar inteligencia), encriptando archivos y exigiendo el pago de 4 millones dólares. Ante la negativa de pago, se filtraron en la Deep Web alrededor de 2000 archivos, que representan aproximadamente al 5% de los archivos robados[11].

V.ii.Brasil

Según Kaspersky, Brasil es uno de los principales hogares de los más activos y creativos cibercriminales[12]. Los ataques que están dirigidos a herramientas de acceso remoto aumentaron un 333% entre febrero y abril del corriente año. Entre las empresas víctimas, se encontraron CPFL Energia, Cosan, Aliansce Sonae, Arteris y la empresa portuguesa EDP, que opera en el sector eléctrico en Brasil. Sólo en abril de este año, Brasil fue blanco de más del 60% de los ataques que la empresa identificó que se realizaron en América Latina. De acuerdo con un informe de la empresa, dos de cada tres (67%) empleados que trabajan desde casa en Brasil aún no han recibido ninguna orientación específica o capacitación de seguridad informática.

En relación a los más afectados por troyanos bancarios móviles, Brasil se encuentra en el Top 10 de esta lista a nivel global, ocupando el cuarto lugar. Además, durante el primer semestre, malwares disfrazados de aplicaciones educativas (como Zoom, Meet, etc) aumentaron al punto de convertirse en el quinto país más atacado a nivel mundial.

Tras el gran incremento de ciberataques a agencias de gobierno y organismos privados, Sabbat, director del GSI, anunció en el Cyber Security Summit Brasil 2020 la creación del Plan Nacional de Gestión de Incidentes Cibernéticos como un avance para la ciberseguridad nacional, con el objetivo de reducir la cantidad de ataques cibernéticos contra ciudadanos e instituciones, trabajando en conjunto con organismos públicos y privados. Además sostuvo que proyecta crear un Sistema de Gestión de Incidentes Cibernéticos, en conjunto con un Decreto del Poder Ejecutivo instituido dentro de la Política Nacional de Ciberseguridad.

V.iii.Chile

En la lucha contra el coronavirus, el Ministerio del Interior y Seguridad Pública de Chile se han encargado de alertar sobre los riesgos cibernéticos asociados a esta crisis, además de activar la agenda de la digitalización. Entre enero y junio de este año, tuvo 525 millones de intentos de ciberataque. Esta cifra ilustra la realidad que, tanto el país andino como el resto del

[11] Brodersen, J., Blanco P. J., 10 de septiembre de 2020

[12] https://www.kaspersky.com/about/press-releases/2020_tetrade-brazilian-cybercriminals-take-the-next-generation-of-banking-malware-global

mundo, han estado experimentando a lo largo de los últimos años, sin mencionar el auge de esta tendencia en los meses de pandemia. El Gobierno de Piñera entiende que la crisis sanitaria profundizó el proceso de digitalización del país, volviendo cada día más urgente adoptar nuevas tecnologías que consideren la seguridad como un elemento fundamental para proteger los datos e información de las instituciones y organizaciones. Las campañas de phishing son la técnica de ataque por excelencia en el mundo cibernético chileno, fomentadas por el encierro, el mayor uso de los correos electrónicos y la curiosidad ciudadana sobre el virus[13].

Las estadísticas realizadas por el Estado chileno también evidencian el aumento de la creación de sitios fraudulentos y ataques por malware y ransomware, aprovechando la coyuntura sanitaria como asunto. Para reflejar la situación, ya en abril se calculó un 20% de aumento de las campañas de phishing en Chile en los últimos meses, siendo los rubros más afectados los bancos, servicios de streaming, supermercados y plataformas de correo. Asimismo, el CSIRT detectó 312 sitios fraudulentos que utilizaron el concepto COVID-19 solamente en abril (un 700% más con respecto a marzo). De esta manera, se consuman múltiples ataques contra la disponibilidad de los servicios en sitios web del sistema de salud con objeto de obtener ganancias económicas *(Equipo de Respuesta ante Incidentes de Seguridad Informática, 2020)*

De este modo, la pandemia puso a prueba el real compromiso estatal con la ciberseguridad. Para esto, el CSIRT dispone de una serie de protocolos e instrumentos de comunicación, que contienen un análisis de los riesgos cibernéticos asociados al COVID-19 *(Equipo de Respuesta ante Incidentes de Seguridad Informática, 2020*). Por tanto, se han llevado a cabo numerosas actividades respecto a la promoción de la seguridad cibernética y prevención de los ataques informáticos. Mediante los distintos organismos especializados en la seguridad cibernética, el Gobierno acerca a la sociedad todo tipo de recomendaciones para prevenir ataques informáticos durante la nueva normalidad. Por ejemplo, el CSIRT han elaborado guías con consejos de seguridad para llevar a cabo las videoconferencias, para una navegación en Internet segura, sobre cómo evitar robots y fraudes en el e-commerce, cómo evitar ser víctima de un delito informático, malware, y cómo prevenir riesgos y lograr mantener una continuidad laboral segura desde los hogares, entre otras. El 29 de abril, en una reunión que el Gobierno abordó los riesgos informáticos en el contexto de la pandemia, se dio a conocer la creación de "La Campana", una herramienta de detección que permite alertar cuando es inscrito en el Network Information Center (NIC) -operador de registro de los dominios de nivel superior del sistema de nombres de dominio de Internet- un sitio de nombre similar a una organización

[13]Un ejemplo de cómo el encierro y la desinformación ayudan a crear el ambiente para la estafa, se puede extraer de un correo de phishing donde el atacante se hace pasar por el Banco de Chile -uno de los bancos con mayor reputación y con más clientes en el país-. El mensaje destaca el compromiso de la entidad bancaria con la salud, utilizando como señuelo un enlace que permite autorizar la postergación del pago de créditos y otros servicios desde los hogares.

específica. En julio, el Comité Interministerial aprobó ocho medidas a efectos de fortalecer los proyectos de seguridad cibernética. Durante esta sesión, se han abordado tres temas principales relacionados a la revisión del estado de avance de todas las medidas de ciberseguridad realizadas hasta la fecha en base a la Política Nacional de Ciberseguridad, el plan de trabajo programado hasta marzo del año 2022, y una serie de medidas aprobadas con acción inmediata. Algunos puntos importantes de esta última son la elaboración del Instructivo de Ciberseguridad en materia de Teletrabajo y trabajo a distancia con recomendaciones y buenas prácticas relacionadas con la ciberseguridad en este ámbito; la conformación de un equipo de trabajo para la revisión multisectorial del proyecto de Ley Marco de Ciberseguridad y de Infraestructura Crítica de la Información; y la celebración de nuevos Convenios de Cooperación de Ciberseguridad estratégicos para el país.

El Gobierno de Chile ha manifestado su intención de proliferar su proceso nacional de digitalización. Incluso, a raíz de la pandemia, la digitalización se ha intensificado en las vidas de los ciudadanos con mayor celeridad y dependencia. Sin embargo, el pasado agosto el CSIRT, en su revista "Cibersucesos", abordó la situación de las personas de tercera edad en la era digital, especialmente durante la profundización forzada de la digitalización en el país. Para las generaciones mayores, hijos del uso de sistemas analógicos, el salto a la digitalización implica superar una serie de barreras de lenguaje y pensamiento. Las condiciones excepcionales de esta pandemia han precipitado a esta generación a dos alternativas posibles: la resignación o la reinvención. El Gobierno entiende fundamental crear motivaciones y competencias, para que este grupo de la sociedad tome conciencia de las ventajas que ofrece la tecnología en términos de satisfacer sus necesidades cotidianas. Un elemento central en esa educación es la sensación de seguridad al momento de utilizar plataformas y dispositivos electrónicos, la cual actúa como catalizador del cambio (Equipo de Respuesta ante Incidentes de Seguridad Informática, 2020). Este aspecto del asunto es relevante para Chile en especial, ya que la longevidad promedio de la sociedad lo sitúa en un estado de envejecimiento moderado a avanzado.

V.iv.Paraguay

En junio, el Viceministro del Ministerio de Tecnologías de la Información y Comunicación (MITIC), Miguel Martin, explicó que el gran limitante de Paraguay en materia digital es su infraestructura de conectividad, por lo que aseguró que desde la cartera de Tecnologías se está trabajando para disponer y definir políticas de conexión adecuadas (Agencia de Información Paraguaya, 16 de junio). En ese contexto, destacó que la app CovidPy fue implementada desde los primeros días de la propagación del coronavirus en el país. Esta aplicación está a cargo de la Dirección de Vigilancia de Salud. A la fecha, cuentan con dos herramientas claves que conectan al Gobierno Nacional con la ciudadanía: el portal de la

Contraloría y Rendición de Cuentas -elaborados por el MITIC- "representan una política de transparencia importante ante los gastos e inversiones que están naciendo en el marco de la pandemia" expresó el funcionario. Como respuesta a las necesidades que surgieron debido a las medidas sanitarias adoptadas, se contempla desde el MITIC crear una red nacional que de proporcione un expediente electrónico en todos los ministerios del Poder Ejecutivo.

Con la finalidad de promover la innovación en la gestión pública mediante el uso y aprovechamiento de la tecnología, el MITIC lanzará el primer Laboratorio de Gobierno denominado GobLab Paraguay, en el marco de la Agenda Digital. El diseño de este proyecto fue desarrollado por el equipo técnico del MITIC en conjunto con el Banco Interamericano de Desarrollo (BID) y la prestigiosa Universidad de Nueva York. Los estudios preliminares revelaron que el conocimiento de las habilidades de innovación en el sector público de Paraguay es mejorable. Esta realidad apunta a un avance del GobLab, el cual pretende adaptarse a las necesidades formativas y organizativas, además de permitir co-construir soluciones tanto testeadas como validadas para un problema público (Agencia de Información Paraguaya, 3 de septiembre). Este primer Laboratorio de Gobierno busca articular una nueva relación entre el Estado y los ciudadanos a través de un servicio ágil y flexible que apunte hacia la construcción de soluciones, testeadas y validadas, para un problema público (Agencia de Información Paraguaya, 8 de septiembre).

V.iv. Uruguay

Durante el año 2020 el Estado uruguayo ha demostrado que la ciberseguridad no ha dejado de ser un tema en su agenda, mostrando avances y novedades en esta área. El 7 y 8 de septiembre de este año Mauricio Papaleo, director del área de Seguridad de la Información de AGESIC junto a Ignacio Lagomarsino, gerente del CERT-UY participaron de las primeras Jornadas del Polo Binacional Educativo Científico Tecnológico Salto Grande. Durante estas jornadas, dedicadas a debatir y presentar herramientas para impulsar el desarrollo del país en un escenario post pandémico mediante la transformación digital, la innovación y la ciberseguridad, los funcionarios expusieron sobre el estado actual de la materia de seguridad de la información en el Uruguay. Asimismo, señalaron que el mayor desafío actual que enfrenta el país es la formación de profesionales competentes que satisfagan la gran demanda proveniente del sector privado (Centro Nacional de Respuesta a Incidentes de Seguridad Informática de Uruguay, 2020).

Un importante anuncio acaecido también durante el 2020 es la firma del contrato de adhesión entre la AGESIC y Ceibal para la creación y funcionamiento de un Centro de Operaciones de Ciberseguridad Gubernamental (GSOC) en el marco del Plan Ceibal. Este organismo contaría con servicios de monitoreo avanzado para permitir el constante análisis en

tiempo real de activos críticos, facilitando la detección temprana de posibles incidentes de seguridad (Centro Nacional de Respuesta a Incidentes de Seguridad Informática de Uruguay, 2020). Este proyecto se enmarca en el préstamo otorgado por el Banco Interamericano de Desarrollo (BID) a Uruguay durante el año 2019 para mejorar las capacidades operativas del CERT-UY. Se estima que el Estado uruguayo lleve adelante otras 17 iniciativas entre el 2020 y el 2023 en diversos organismos y sectores públicos para incrementar sus capacidades de ciberseguridad a nivel nacional.

VI. Reflexiones finales

- **Claridad conceptual operativa:** En la variable gubernamental analizada - el proyecto institucional -, se han puesto en evidencia a lo largo de este trabajo los avances en los últimos veinte años en materia de ciberseguridad. Sin embargo, aún es posible encontrar cierta oscuridad conceptual para desagregar los incidentes, delitos y ataques cibernéticos (Núñez, 2019). Esto se ve agravado ante la falta de datos, a la cual este trabajo se referirá en el siguiente subapartado.
- **Centros de Respuesta:** Es preciso destacar que la creación de Centros de Respuesta en el Cono Sur no necesariamente se realizó en el marco de la ENSC. En algunos casos (Argentina; Paraguay; Uruguay) los Centros fueron creados con anterioridad. Esta observación supone considerar seriamente el rol de los organismos internacionales en el proceso de formulación y robustecimiento de estrategias en materia de ciberseguridad que condujeron a las ENSC actuales y futuras.
- **Ciberataques:** El incremento de los ciberataques en los últimos meses puede ser un acontecimiento fundante para repensar la prioridad dada a la ciberseguridad, de la misma manera en que los "Mega-Eventos" llevaron a que Brasil impulse una primera estrategia coordinada, la región puede aprender la lección en este momento[14].
- **La falta de datos:** Deviene fundamental hacer hincapié en el problema de la falta de información oficial y confiable. En un sector que se caracteriza por la falta de transparencia (los actores privados evitan hacer públicos los incidentes cibernéticos para proteger su reputación**,** falta de presupuesto público), es fundamental que los Estados primero cuenten con la capacidad de recolectar la información sobre los incidentes cibernéticos, y segundo, que lo hagan de forma pública. La ausencia de datos oficiales actualizados y confiables representa un problema para conocer el estado real de la cuestión. Así, por ejemplo, pese a existir datos públicos del plan integral de la ENSC (el primero de los microindicadores del proyecto institucional), no existen datos públicos sobre bienes y servicios brindados en relación con las competencias institucionales y el

[14] Equipe Artigo 19, 2016.

plan expresado (el segundo de los microindicadores del elemento proyecto institucional). Esto, a su vez, representa un obstáculo para implementar las políticas públicas adecuadas. El caso de Argentina es paradigmático. Carece de una fuente pública de datos sobre los delitos sucedidos en los últimos años, y su principal Centro y Equipo de Respuesta ante Incidentes de Seguridad Informática - el ICIC-CERT-, a diferencia del resto de los países del Cono Sur, no cuenta con una página web propia.

- ➔ **Los desafíos de la pandemia**: La pandemia puede representar un momento bisagra para la seguridad informática en la región. Ha quedado en evidencia el rol preeminente de las nuevas tecnologías en las sociedades del Cono Sur, tanto para el funcionamiento de los Estados como para sostener la vida socio-económica de la población. Las consecuencias sobre las infraestructuras críticas quedaron expuestas a la necesidad de promover un debate abierto, que incluya a diversos sectores de la sociedad civil y a otros actores estatales, sobre el camino a seguir con respecto a la seguridad informática. La cooperación entre actores estatales, empresas, ONGs y la sociedad civil será probablemente fundamental para una ciberseguridad regional integral.

Bibliografía

Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento (2019, 23 de septiembre). *Agenda Digital del Uruguay*. https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/politicas-y-gestion/programas/agenda-digital-del-uruguay

Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento (2020, 11 de marzo). *Marco de Ciberseguridad*. https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/publicaciones/marco-ciberseguridad

Agencia de Información Paraguaya (2020, 16 de junio). *Presentan acciones y resultados obtenidos sobre el uso de tecnología durante la pandemia*. https://www.ip.gov.py/ip/presentan-acciones-y-resultados-obtenidos-sobre-el-uso-de-tecnologia-durante-pandemia-covid-19/

Agencia de Información Paraguaya (2020, 3 de septiembre). *Mitic avanza en la creación del primer Laboratorio de Gobierno para la innovación pública.* https://www.ip.gov.py/ip/mitic-avanza-en-la-creacion-del-primer-laboratorio-de-gobierno-paraguay/

Agencia de Información Paraguaya (2020, 8 de septiembre). *GobLab Paraguay busca la digitalización e innovación en la administración pública.* https://www.ip.gov.py/ip/goblab-paraguay-busca-la-digitalizacion-e-innovacion-en-la-administracion-publica/

Argentina.gob.ar. (2020, 16 de julio). *1ª reunión 2020 de Comisión de Infraestructura Tecnológica y Ciberseguridad del COFEFUP*. https://www.argentina.gob.ar/noticias/1a-reunion-2020-de-comision-de-infraestructura-tecnologica-y-ciberseguridad-del-cofefup

Banco Interamericano de Desarrollo y Organización de los Estados Americanos (2020). *Reporte: Ciberseguridad: Riesgos, Avances y el camino a seguir en América Latina y el Caribe*. Observatorio de ciberseguridad. https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf

Bernazza, C. ; Longo, G.; Comotto, S. (2015). *Evaluando en clave pública : guía de instrumentos e indicadores para la medición de capacidades estatales*. 1a ed. - Ciudad Autónoma de Buenos Aires: Flacso Argentina.

Brodersen, J., Blanco P. J. (2020, 10 de septiembre) Ciberataque a Migraciones: qué información robaron y publicaron los ciberdelincuentes. *Clarín.*

https://www.clarin.com/tecnologia/ciberataque-migraciones-informacion-robaron-publicaron-ciberdelincuentes_0_Pfe1OVNlI.html

Centro Nacional de Respuesta a Incidentes de Seguridad Informática de Uruguay (2020, 8 de septiembre). *Ciberseguridad: educación y buenas prácticas de las organizaciones.* https://www.gub.uy/centro-nacional-respuesta-incidentes-seguridad-informatica/comunicacion/noticias/ciberseguridad-educacion-buenas-practicas-organizaciones

Centro Nacional de Respuesta a Incidentes de Seguridad Informática de Uruguay (2020, 21 de septiembre). *Plan Ceibal contará con un Centro de Operaciones de Ciberseguridad gubernamental*. https://www.gub.uy/centro-nacional-respuesta-incidentes-seguridad-informatica/comunicacion/noticias/plan-ceibal-contara-centro-operaciones-ciberseguridad-gubernamental

Corporación Andina de Fomento - Banco de Desarrollo de América Latina (2017) *Hacia la transformación digital de América Latina y el Caribe:El Observatorio CAF del Ecosistema Digital.* https://scioteca.caf.com/bitstream/handle/123456789/1059/Observatorio%20CAF%20del%20ecosistema%20digital.pdf?sequence=7&isAllowed=y

Equipe Artigo 19 (2016). *DA CIBERSEGURANÇA À CIBERGUERRA. O desenvolvimento de politicas de vigilância no Brasil.*

Equipo de Respuesta ante Incidentes de Seguridad Informática (2020). Ciberbullying y grooming. *Ciber Sucesos, Vol N°2*. https://www.csirt.gob.cl/media/2020/08/Cibersucesos-n%C2%B02.pdf

Equipo de Respuesta ante Incidentes de Seguridad Informática (s.f.), *Comité Interministerial aprueba 8 medidas para fortalecer proyectos de ciberseguridad*, Noticias. https://www.csirt.gob.cl/noticias/comite-interministerial-aprueba-8-medidas-para-dar-continuidad-y-fortalecer-proyectos-de-ciberseguridad/

Equipo de Respuesta ante Incidentes de Seguridad Informática (2020, 4 de septiembre), *Propuesta de trabajo sobre marco regulatorio marca la pauta en cuarto Comité Interministerial de Ciberseguridad*, Noticias. https://www.csirt.gob.cl/noticias/cics4/

Equipo de Respuesta ante Incidentes de Seguridad Informática (2020). Riesgos cibernéticos del COVID-19. *Ciber Sucesos Vol. N°1*. https://www.csirt.gob.cl/media/2020/07/Cibersucesos.pdf

Gobierno de Chile (2015), *Política Nacional de Ciberseguridad*. https://www.ciberseguridad.gob.cl/media/2017/05/PNCS-ES-FEA.pdf

Gomez Vieites, A. (2011), *Enciclopedia de la seguridad informática*. Alfaomega Grupo Editor.

Hathaway, M.; Demchak C., Kerben, J; McArdle, J; y Spidalieri, F. (2015), *A Plan for Cyber Readiness: A baseline and Index. Cyber Readiness Index 2.0.* Potomac Institute for Policy Studies. https://www.potomacinstitute.org/images/CRIndex2.0.pdf

International Telecommunication Union (2020) *World Telecommunication/ICT Indicators Database 2020.* https://www.itu.int/en/ITU-D/Statistics/Pages/publications/wtid.aspx

International Telecommunication Union. (2019). *Measuring digital development. Facts and figures*. https://www.itu.int/en/ITU-D/Statistics/Documents/facts/FactsFigures2019.pdf

Lacalle Pou (2020) *Discurso ante la 75° Asamblea General de la Organización de las Naciones Unidas*. https://www.nodal.am/2020/09/uruguay-discurso-del-presidente-luis-lacalle-pou-en-la-75o-asamblea-general-de-onu/

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.*

Luiijf, E.; Besseling, K.; De Graaf, P. (2013). Nineteen national cyber security strategies. *International Journal of Critical Infrastructures.*

Matus, C. (1987). *Política, planificación y gobierno*. Caracas: Fundación ALTADIR.

TÉLAM. (2020, 16 de julio) El Gobierno analiza con empresas privadas estrategias de ciberseguridad preventiva. *TÉLAM*. https://www.telam.com.ar/notas/202007/485583-gobierno-analiza-empresas-privadas-estrategias-ciberseguridad-preventiva.html

Observatorio Corporación Andina de Fomento del Ecosistema Digital (2020) *El estado de la digitalización de América Latina frente a la pandemia del COVID-19.* https://scioteca.caf.com/bitstream/handle/123456789/1540/El_estado_de_la_digitalizacion_de_America_Latina_frente_a_la_pandemia_del_COVID-19.pdf