Ciberseguridad en Uruguay

Análisis a la luz de la Estrategia Interamericana Integral para Combatir las Amenazas a la Seguridad Cibernética

María Fernanda González Hernández
CI 4.797.762-0

Tutor: Mag. Mónica Nieves

Monografía Final de Investigación de Grado en Relaciones Internacionales

2019
Facultad de Derecho
Universidad de la República

Índice

Resumen

Este trabajo de investigación se enfoca en la temática de la ciberseguridad en el Uruguay, centrándose principalmente en la Estrategia Interamericana de Ciberseguridad de la OEA y el grado de influencia que ésta ha tenido en el país.

Mediante un análisis bibliográfico, se realiza un estudio sobre la ciberseguridad a nivel regional para luego describir en profundidad la Estrategia de la OEA. A partir de dicho estudio, se busca determinar si esta tuvo aplicación en Uruguay y las diferentes formas en que se llevó a cabo la adaptación de las recomendaciones de dicho instrumento a la realidad nacional. Otro de los objetivos del presente trabajo es analizar el plan de acción de Uruguay en ciberseguridad.

Palabras clave: Ciberseguridad, OEA, Estrategia, Amenazas, Seguridad Cibernética, Uruguay.

Introducción

Hoy en día, no cabe duda de que la tecnología ha demostrado ser un gran aliado de la economía mundial, la democracia y los Estados. Sin embargo, como sucede con muchas otras herramientas al servicio del hombre, también su uso se ha visto redireccionado maliciosamente por actores que buscan provecho económico o en ocasiones, simplemente hacer daño.

Internet y las tecnologías de la información han catapultado las economías nacionales, y en muchos casos han promovido el acceso a la democracia y los derechos de las personas. Esto implica que mucha información sensible tanto a nivel estatal como empresarial y personal se ha visto expuesta a nuevas modalidades delictivas que atentan contra estos actores. Destrucción o manipulación de datos almacenados en la red han dificultado las funciones de los gobiernos y generado pérdidas económicas incalculables, sin mencionar la invasión a la privacidad y el efecto de desconfianza y temor a las redes que genera en los usuarios. Internet como red que posibilita transacciones para individuos y entes gubernamentales y empresariales es considerado una herramienta al servicio de estos, pero su uso de forma malintencionada genera amenazas para los usuarios. Otro efecto de esta situación es el recelo que se genera sobre su uso y esto no le permite alcanzar un mayor potencial como instrumento de la sociedad.

Por todo lo planteado anteriormente, se entiende que la ciberseguridad es un tema de actualidad con una gran relevancia a nivel global. Involucra a diferentes actores internacionales, y no darle la importancia necesaria puede tener efectos altamente negativos tanto para un Estado, como una empresa e individuos en general.

Si bien ha habido un involucramiento activo por parte de los Estados y los organismos internacionales durante los últimos años en esta temática, el ritmo vertiginoso en el que se desarrollan la tecnología y las redes generan a su vez nuevas amenazas constantes que dificultan la tarea de mantener la seguridad cibernética. Otro aspecto no menor es el carácter relativamente novedoso, tanto del internet y las redes como de las estrategias internacionales y regulaciones estatales que buscan reglamentarlas. Esto genera que la literatura o investigación existente también esté en constante desarrollo y sean contados los estudios especialmente dedicados a dicha materia para el ámbito regional. El Programa de Seguridad Cibernética de la OEA comenzó en 2013 a generar documentación y reportes sobre la situación regional en

seguridad cibernética, y ha constituido un gran esfuerzo por brindar una visión global del posicionamiento de América del Sur y el Caribe en esta temática. Sin embargo, no ha sido exhaustivamente estudiada la repercusión de la Estrategia Interamericana de Seguridad Cibernética a nivel nacional, específicamente para el caso de Uruguay.

Este trabajo de investigación realiza un análisis de la situación general en materia de ciberseguridad a nivel regional, para luego profundizar en el estudio de la Estrategia Interamericana de Seguridad Cibernética de la OEA y el alcance o influencia que ha tenido ésta en Uruguay. Se describirán en profundidad los lineamientos de dicho Estado en ciberseguridad, y las diferentes iniciativas y acciones gubernamentales en la materia. Se trata de una primera aproximación a un tema de gran complejidad, con múltiples aristas.

La principal motivación de esta investigación es comprender el panorama actual en la región en lo que refiere a la ciberseguridad, y determinar el grado de influencia de la Estrategia Interamericana de la OEA en el accionar gubernamental de Uruguay y la generación de políticas públicas afines.

a. Problema de investigación

El problema o pregunta de investigación del presente trabajo es el siguiente: ¿Han influido los planteos de la Estrategia Interamericana de Seguridad Cibernética de la OEA en la generación de medidas de Uruguay en materia de ciberseguridad? De ser así, ¿en qué grado se han cumplido las recomendaciones esbozadas en dicha Estrategia?

El período de estudio seleccionado comprende desde el año 2004 (año en que se aprobó la Estrategia de la OEA) al 2018.

b. Objetivos

Objetivos generales y específicos

Generales:

1) Determinar la influencia de la Estrategia desarrollada por la OEA, en los lineamientos en ciberseguridad seguidos por Uruguay

2) Identificar el plan de acción de Uruguay en materia de ciberseguridad, y los actores involucrados

Específicos:

Describir en detalle el programa estatal en materia de ciberseguridad

Comparar las recomendaciones expuestas en la Estrategia Interamericana Integral de Seguridad Cibernética con el accionar gubernamental del Estado uruguayo en dicha materia, como ser: la creación de organismos, formulación de leyes, entre otras medidas.

Comparar dicho accionar estatal con las medidas en ciberseguridad realizadas en otros Estados de la región.

Analizar el posicionamiento de Uruguay en dicha temática a nivel regional

c. Aspectos metodológicos

Este trabajo se basa en un enfoque cualitativo, de naturaleza bibliográfica. Se realiza un estudio descriptivo del objeto de estudio, tomando como tema global la ciberseguridad y la Estrategia Interamericana de Seguridad Cibernética de la OEA, y llevándolo de lo general (el panorama regional) a lo particular (Uruguay).

Mediante la comparación de diferentes fuentes de información primaria y secundaria, se realiza una investigación documental. Para esto se utilizaron documentos oficiales de organismos internacionales y entes gubernamentales, junto con artículos periodísticos y otros trabajos de investigación. A partir de esta información, se identificó el panorama actual en el contexto regional, tomando a su vez dos Estados (Chile y Brasil) para ejemplificar la diversidad de situaciones que existen en continente. La elección nace de un criterio fundamental que es mencionado durante el presente trabajo: la presencia o ausencia de una Estrategia Nacional de Ciberseguridad. Esto es lo que determinará, entre otros factores, el nivel de preparación de dicho Estado frente a las amenazas cibernéticas.

d. Estructura

El análisis se presenta en cuatro capítulos, el primero refiere a los antecedentes del tema seleccionado y el marco conceptual y teórico en el que se basará el presente trabajo. El segundo capítulo se dedica a analizar la ciberseguridad en la región, y toma dos Estados como ejemplos para comparar los diferentes niveles de seguridad cibernética que existen.

Luego, el tercer capítulo realiza una descripción detallada de la Estrategia Interamericana de Ciberseguridad de la OEA, y a partir de cada planteo de la misma, analiza en qué grado se vio reflejada en Uruguay. En el cuarto y último capítulo, se examina el plan de acción de Uruguay en seguridad cibernética, tomando en cuenta todos los instrumentos y herramientas jurídicas que se han llevado adelante hasta la fecha, para luego estudiar la puesta en práctica de los mismos.

Por último, se presentan las consideraciones finales a modo de conclusión para dar un cierre de reflexión y plantear los hallazgos de la presente investigación.

Capítulo I

Antecedentes

Las redes de información han trascendido fronteras, desdibujando los límites políticos y conectando individuos y organizaciones en todo el mundo, haciendo posible el fenómeno de la globalización. Teniendo en cuenta esta característica, las amenazas que se generan son de aún mayor magnitud y con mayor potencial de daño.

Organismos internacionales y regionales se han abocado a la misión de proteger la información, considerada como un activo fundamental para los Estados, tomando como propia la misión de incentivar la seguridad cibernética y prevenir los delitos informáticos que puedan poner en jaque dicho activo. La Organización de Naciones Unidas (ONU) contempló este fenómeno en su 12º Congreso sobre Prevención del Delito y Justicia Penal realizado en Salvador (Brasil), en abril de 2010. En dicho evento, se trató la importancia de contener la “ciberdelincuencia”, resaltando la necesidad de un marco jurídico apropiado y un accionar conjunto. La protección de la seguridad

internacional es el primer propósito esgrimido en la Carta de la ONU. Dicho esto, la seguridad de los Estados involucra muchos aspectos, entre los que se incluye la seguridad de la información, hoy contenida mayormente en el ciberespacio.

Por su parte, la Organización de Estados Americanos (OEA) contempla a la seguridad como uno de sus pilares fundamentales de acción. Con este fin, constituyó la Secretaría de Seguridad Multidimensional (SSM)[1] de la que forma parte el Comité Interamericano contra el Terrorismo (CICTE). Este organismo busca combatir y prevenir el terrorismo, mediante la cooperación entre los Estados miembros, y uno de sus programas está dedicado a seguridad cibernética. Cabe mencionar que las amenazas a la seguridad cibernética fueron identificadas por dicha organización como una de las amenazas terroristas emergentes. Es en el marco de esta estructura, que se aprueba en 2004 la resolución AG/RES. 2004 (XXXIV-O/04) en la Asamblea General de la OEA, la cual consiste en la "Estrategia Interamericana Integral para Combatir las Amenazas a la seguridad cibernética" que se desarrollará en el presente trabajo, y es el documento que le brinda el marco a la Secretaría del CICTE para actuar en temas de ciberseguridad.

La OEA insiste en que la tarea de proteger los activos cibernéticos se debe encauzar de forma masiva y contemplando a todos los actores, mediante un enfoque integral e internacional. Un solo Estado u organización no puede hacer frente a estas amenazas transnacionales. El esfuerzo debe ser conjunto y multilateral, mediante la cooperación entre Estados, y dentro de éstos, la cooperación entre sectores públicos y privados (OEA, 2004). Así se manifestó en la web principal de la OEA dedicada a la seguridad cibernética, más específicamente del CICTE:

> La Secretaría del CICTE emplea un enfoque integral en la construcción de capacidades de seguridad cibernética entre los Estados Miembros, reconociendo que la responsabilidad nacional y regional para la seguridad cibernética cae sobre una amplia gama de entidades tanto del sector público como el privado, los cuales trabajan en aspectos políticos y técnicos para asegurar el ciberespacio (OEA, 2018).

[1] Este organismo fue creado en el año 2005 dentro de la órbita de la OEA.

El mismo concepto se ve expresado en el informe del 2016 sobre ciberseguridad del Banco Interamericano de Desarrollo (BID) en conjunto con la OEA, titulado "Ciberseguridad: ¿estamos preparados en América Latina y el Caribe?" (BID, OEA, 2016). En él, se afirma que "en la actualidad se entiende que el delito cibernético no reconoce fronteras nacionales y que se requiere un esfuerzo multilateral y multidimensional para abordar la cantidad de amenazas informáticas" (Banco Interamericano de Desarrollo, 2016, p. XI).

Como antecedente que funcionará a modo de marco para este proyecto final, se utilizará el informe[2] sobre ciberseguridad elaborado por la OEA y el BID, mencionado anteriormente. Dicho informe estudia en profundidad la capacidad de la región en ciberseguridad, la confianza y privacidad en las redes, legislación y capacidad de respuesta, entre otros temas. Finalmente realiza un perfil por Estado en el cual, de forma resumida, se caracteriza a cada uno de ellos de acuerdo a su desarrollo en ciberseguridad, considerando múltiples factores previamente conceptualizados.

Esta investigación reúne valiosísima información sobre el contexto regional, y ofrece una visión general de cada Estado de la región. Sin embargo, no se han desarrollado estudios que profundicen sobre la situación actual de Uruguay en esta materia, y más específicamente en cómo se ha aplicado la Estrategia de Ciberseguridad de la OEA desde su publicación en el 2004.

Existen otros antecedentes de estudios vinculados a la ciberseguridad y centrados en otras regiones u organizaciones internacionales que, si bien no aportan conocimientos específicos sobre la posición de Uruguay ni la OEA en este tema, sí proveen un acercamiento a cómo otros Estados y actores trasnacionales enfrentan en conjunto esta problemática. Es el caso de la publicación titulada "La ciberseguridad como factor crítico en la seguridad de la Unión Europea", de Machín y Gazapo (2016). Se centra en cómo la ciberseguridad es fundamental para varios sectores productivos y servicios de los Estados, y las líneas de acción y evolución de la Estrategia de Ciberseguridad europea.

Por su parte, Leiva (2015) se dedica a analizar y comparar diferentes casos de Estrategias Nacionales de Ciberseguridad, identificando los principales puntos abarcados por dichas estrategias, los factores de riesgo y los déficits en cómo enfrentan

[2] Último informe publicado por dichos organismos dentro del período de estudio del presente trabajo.

las naciones el desafío de la ciberseguridad. De acuerdo con dicho estudio, con respecto a los Estados de Latinoamérica, la mayor parte de estos tienen establecidos sus propios Equipos de Respuesta ante Emergencias Informáticas, en inglés *Computer Emergency Response Team* (CERTs), que brindan respuesta a incidentes a nivel nacional. El grado de desarrollo de estos centros es diverso, ya que algunos previenen y responden a incidentes mientras otros aún no han logrado proteger efectivamente sus redes (Leiva, 2015).

El mismo estudio muestra la diferencia que existe entre los procesos de ciberseguridad a nivel mundial: los Estados miembros de la OEA adoptaron la Estrategia Interamericana Integral de Ciberseguridad por unanimidad en 2004, frente a la Unión Europea que lo cumplió finalmente en el año 2013. La OEA se constituye como la primera organización internacional de carácter regional en presentar una Estrategia de Ciberseguridad. Un documento relevante a tener en cuenta es la Declaración del "Fortalecimiento de la Ciberseguridad en las Américas", de marzo del 2012, el cual busca reafirmar el compromiso de la OEA y sus miembros por cooperar en la prevención y alerta sobre incidentes cibernéticos. Leiva entiende que dicha Declaración deja ver un grado de consenso político entre los Estados, y esto fomenta la cooperación (2015).

A modo general, dos dificultades enfrentan los países latinoamericanos para fortalecer su seguridad informática: la falta de recursos, y la insuficiencia en experiencia y conocimientos técnicos que permitan generar políticas. La asignación de presupuesto para la seguridad informática es generalmente escasa, ya que se priorizan otros aspectos de seguridad (Leiva, 2015).

Marco conceptual

Un concepto fundamental que debe ser definido para poder enmarcar el presente trabajo de investigación es el delito informático. Es un fenómeno que, en sus comienzos, lógicamente por su novedad no estaba incluido en las figuras típicas legales de los regímenes jurídicos nacionales, y llevaba a los Estados a tipificarlo dentro de algún tipo de delito tradicional ya existente. Sin embargo, el aumento del uso de la

tecnología y las redes generó además el incremento de su uso indebido, factor que favoreció la regulación de esta nueva modalidad de crímenes. En el ámbito internacional no existe una definición consensuada de delito informático, pero se han desarrollado varias nociones de carácter nacional, al tiempo que la ONU y la OEA delimitaron el concepto para poder trabajar en ciberseguridad.

A los efectos de delimitar el concepto para este trabajo, se les considerará como cualquier delito que haya involucrado un equipo, dispositivo de hardware o red para cometerlo (Ojeda, Rincón, Arias, Daza, 2010). Es una definición simplificada de un fenómeno complejo, que puede tener manifestaciones diversas. Otra definición a tener en cuenta afirma que "el delito informático es toda conducta ilícita, ya sea por acción u omisión, que realiza una persona mediante el uso de cualquier recurso informático y que, como consecuencia, afecta un bien informático jurídico y/o material que se encuentra legalmente protegido, haciéndose penalmente responsable por tal hecho" (Ojeda, et al., 2010). Una tercera definición que considerar es la que acuña el Dr. Santiago Acurio del Pino[3]: "delincuencia informática es todo acto o conducta ilícita e ilegal que pueda ser considerada como criminal, dirigida a alterar, socavar, destruir, o manipular, cualquier sistema informático o alguna de sus partes componentes, que tenga como finalidad causar una lesión o poner en peligro un bien jurídico cualquiera". (Acurio del Pino [s.f]).

El Diccionario Latinoamericano de Seguridad y Geopolítica, de Miguel Ángel Barrios (2009) define al cibercrimen como "el delito que viola la seguridad de internet mediante la utilización de software malicioso, denominado malware, por el desarrollo de una actividad criminal (…)". A su vez, ahonda en la descripción del funcionamiento de este tipo de delitos, señalando que estas violaciones cibernéticas se producen en su mayoría mediante redes de programas denominados *botnets*, cuya función es "enviar *spam* o alterar los servicios mediante 'gusanos' portadores de programas que pasan de una computadora a otra y cuya presencia es desconocida por los usuarios porque es prácticamente invisible para el software comercial antivirus" (Barrios, 2009).

Se conocen diferentes clases de delitos informáticos. A modo de ejemplo, la ONU reconoce cuatro tipos: los cometidos mediante manipulación de computadoras (incluye datos de entrada, programas, datos de salida y procesos), las falsificaciones

[3] Profesor de Derecho Informático de la Pontificia Universidad Católica del Ecuador

informáticas (como objeto o instrumento), los daños o cambios a programas o datos (el sabotaje informático, los virus, gusanos, bombas lógicas) y por último, el acceso no autorizado a sistemas y servicios informáticos (protagonizado por piratas y hackers, que pueden reproducir programas sin autorización, por ejemplo). (Hall, s.f)

De acuerdo con el CERTuy (2013), un incidente de Seguridad de la Información es “la violación o amenaza inminente a la Política de Seguridad de la Información implícita o explícita”.

Otro concepto fundamental a tener en cuenta, y que se desarrolla a partir de la aparición de dichos delitos informáticos e incidentes, es el de ciberseguridad. “Protección de activos de información**,** a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados” (Asociación de Auditoría y Control de Sistemas de Información, s.f) es una primera aproximación que realiza el ISACA, acrónimo de “Information Systems Audit and Control Association”, y se trata de una organización internacional que busca promover certificaciones y métodos de control de los sistemas informáticos.

Con respecto a este último concepto, Acosta et al. (2009) lo define como “la aplicación de medidas de seguridad para proteger las infraestructuras de los sistemas de información y comunicaciones frente a los ciberataques”.

Barrios (2009) define a la ciberdefensa como “una iniciativa diseñada para ampliar los sistemas de defensa de los Estados y protegerlos de los nuevos riesgos emergentes en la sociedad de la información”. El autor profundiza en este concepto, sumando las redes y sistemas de la información a los conceptos clásicos de defensa vinculados al territorio (tierra, aire y mar). Los considera infraestructura crítica de los Estados.

Es necesario adentrarse en otros conceptos vinculados a la ciberseguridad, que se consideran fundamentales para la investigación que se está llevando a cabo. Es el caso de la Estrategia Nacional de Ciberseguridad, la cual es 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)

Dicha estrategia se entiende como un componente clave en la ciberseguridad estatal, y es establecida como un marco a nivel estratégico desde donde establecer las metas y necesidades nacionales a lograr en determinado tiempo (Leiva, 2015). Participan en ella el gobierno, organismos estatales, organismos reguladores, las industrias y empresas, organizaciones vinculadas al desarrollo e investigación, universidades, y la población en general.

Siguiendo con otras nociones relacionadas a la temática del presente trabajo, cabe mencionar conceptos relevantes como el Gobierno Electrónico y Gobierno en Red. El primero es definido por el Centro Latinoamericano de Administración para el Desarrollo (2007) como:

> El uso de las tecnologías de la información y de la comunicación (TIC) en los órganos de la Administración Pública para mejorar la información y los servicios ofrecidos a los ciudadanos, orientar la eficacia y eficiencia de la gestión pública e incrementar sustantivamente la transparencia del sector público y la participación de los ciudadanos. (p.7)

Por otra parte, el Gobierno en Red es definido como el "entramado de vínculos entre organizaciones, a través de los cuales se prestan servicios, se gestionan actividades y se persiguen objetivos compartidos" (Decreto N° 450/009, 2009). La noción de crear una sociedad conectada, mediante estos vínculos entre las instituciones y la misma es lo que se propone el Gobierno en Red.

Otro concepto relevante para el presente trabajo es el de Política Pública. De acuerdo con el Banco Mundial (2011), una política es un "plan para alcanzar un objetivo de interés público". Se las puede considerar como un conjunto de acciones (que pueden ser programas, reglamentos, estrategias, entre otros) como vías para lograr una meta gubernamental de interés público. Eduardo Sojo (2006) las define como "toda acción de gobierno encaminada a atender o resolver un problema relativo al interés público". Las acciones no están definidas únicamente para el gobierno, sino que por lo general actores del ámbito privado y social también tienen un papel que cumplir, en los lineamientos planteados por la Política Pública.

Marco teórico

Como se mencionó anteriormente, la ciberseguridad ha probado ser un tema de interés internacional e integra cada vez un mayor número de agendas tanto gubernamentales como de organizaciones internacionales. Esto implica que no solo actúan unidades nacionales, si no que otra rama de actores internacionales entra en escena y cumplen un rol cada vez más preponderante. Por este motivo, es que se enmarcará el presente trabajo en un enfoque interdependentista. La teoría de interdependencia compleja, formulada por Keohane y Nye, pone de manifiesto la importancia de los actores no gubernamentales en el ámbito internacional. El Estado nacional se encuentra ahora acompañado de una multiplicidad de actores no territoriales, siendo las organizaciones internacionales el actor al que se le dará mayor protagonismo en este trabajo. Esta teoría busca demostrar que no solo los gobiernos centrales son los que pueden interactuar y realizar proyectos comunes con otros Estados. Ya no es el Estado el actor único e indiscutible de las relaciones internacionales.

Enmarcando dicha teoría en el ámbito del presente trabajo, el panorama actual regional se encuentra protagonizado por la OEA como foro de cooperación entre los Estados y como organización internacional, y se suma así como actor de las relaciones internacionales, junto a los Estados miembros de la misma. En el ámbito regional se identifican entonces tanto Estados nacionales, como organizaciones que tienen poder de decisión y tienen sus propias agendas.

En este sentido, la seguridad cibernética es uno de los programas clave de la OEA, con el que busca coordinar los esfuerzos estatales mediante la Estrategia Interamericana Integral. De acuerdo con el enfoque interdependentista, la necesidad de los Estados por acelerar su progreso y desarrollo los lleva a una cada vez mayor apertura internacional, lo que generalmente trae asociada una dependencia proporcional a la apertura (Nye y Keohane, 1989). Enfocando este concepto al presente trabajo, se podría afirmar que los Estados, en su afán por progresar en materia de seguridad y desarrollar las tecnologías de la información de manera fructífera, acuden a un organismo regional para conseguir su objetivo. Al mismo tiempo, se generaría cierta dependencia de los Estados miembros frente a dicho organismo en la medida que éste les plantea lineamientos a seguir y brinda herramientas para su consecución. Se podría

arriesgar que esto es lo que sucede con la Estrategia de Ciberseguridad que planteó la OEA, y sobre la que se inscribe el presente trabajo.

La interdependencia compleja incluye rasgos de la teoría realista y la modernista, pero llega más allá en su afán por explicar la realidad actual. (Keohane, 1977, p.16). Keohane (1977) entiende que el realismo y la interdependencia no muestran exactamente el panorama mundial en lo política, sino que representan ideales. Las diversas situaciones existentes podrán ubicarse en algún lugar del espectro formado por estas teorías. La interdependencia se da a muchos niveles, siendo los principales el político y el económico.

Otro enfoque de la interdependencia está vinculado a la cooperación entre los entes, en la medida en que la capacidad de uno de ellos de alcanzar su objetivo está subordinada al accionar de otro. Mantienen su autonomía, pero la concreción de sus metas depende de la decisión de los demás. En este sentido, la ciberseguridad (como se planteó anteriormente) es un fenómeno que debe desarrollarse integralmente y desde múltiples enfoques y actores. Las amenazas cibernéticas no conocen de fronteras, y debido a esto, la cooperación entre los Estados miembros de la OEA es fundamental. El perfeccionamiento de la seguridad de las redes debe darse a nivel regional, con la participación de todos. La interdependencia compleja se manifiesta así como paradigma de lo que acontece actualmente a nivel regional en materia de ciberseguridad.

Este enfoque tiene, de acuerdo con lo expuesto por Keohane y Nye (1977), tres rasgos característicos. En primer lugar, las sociedades se encuentran conectadas por canales múltiples, tanto formales como informales (protagonizados por entidades gubernamentales, agencias de servicio exterior, organismos trasnacionales, y élites no pertenecientes al gobierno). Los canales múltiples mencionados serían entonces las relaciones interestatales, transgubernamentales y trasnacionales que se generan entre ellos. Las últimas se presentan cuando los Estados ya no actúan como unidad coherente, y dejan de ser los únicos actores de la realidad mundial. Es donde los supuestos de la interdependencia compleja se manifiestan. En segundo lugar, los varios temas tratados en las agendas de los Estados no están ordenados jerárquicamente, y permite que temas internos se externalicen y viceversa. Por último, la tercera característica indica que entre los gobiernos de una misma región no se aplica la fuerza militar cuando es un escenario de interdependencia compleja. (Keohane, 1977, p.41)

La ciberseguridad podría considerarse inicialmente como un tema de política interna, que se ha visto externalizado mediante la acción de las relaciones transgubernamentales que mantiene cada Estado con la OEA y entre sí. La Estrategia de ciberseguridad que lleva adelante este organismo propone una mirada integral sobre la cuestión, fusionando los cometidos estatales en ciberseguridad para promover una cultura cibernética a nivel regional.

En un marco de interdependencia, las políticas internas nacionales no se encuentran aisladas, si no que están cada vez más conectadas y muchas veces chocan entre sí. La fuerza como instrumento para asegurar la supervivencia de los Estados, un concepto propio de los realistas, es considerado poco adecuado en la visión interdependiente. Existen otros objetivos nacionales, tales como la prosperidad a nivel económico, que están tomando cada vez mayor relevancia y que no pueden ser logrados correctamente a través de la fuerza militar. Aquí es donde entran en acción los organismos internacionales y actores trasnacionales, los cuales son utilizados por los Estados para ejercer el poder y cumplir sus metas. Mediante estos canales de contacto entre los Estados, la política interior y exterior comienza a fusionarse. Las organizaciones internacionales proponen ciertas iniciativas a los gobiernos, teniendo en cuenta para ello los problemas existentes y si existe la posibilidad de que los mismos puedan agruparse; de esta forma, modelan de forma progresiva los intereses estatales y la política interior, al tiempo que fomentan la vinculación de temas.

Como afirman Keohane y Nye (1977), “ellas (las instituciones internacionales) contribuyen, en particular, a establecer la agenda internacional, actúan como catalizadores para la formación de coaliciones y como escenario para iniciativas políticas y vinculación de los Estados débiles”.

La interdependencia compleja proporciona un marco teórico adecuado para encuadrar la presente situación actual en materia de ciberseguridad americana, más específicamente en los países miembros de la OEA. Esta organización ocupa un lugar como actor internacional, junto con los Estados nacionales. Fomentan entre sí relaciones o vínculos, proponiendo iniciativas (como la Estrategia Interamericana Integral para Combatir las Amenazas a la seguridad cibernética) y moldeando las agendas gubernamentales. La OEA no concibe el uso de la fuerza militar entre sus miembros, condena la guerra de agresión y promueve la solución pacífica de controversias.

Otro enfoque teórico que es posible utilizar para la temática del presente trabajo es la vertiente del constructivismo, desarrollada principalmente por Alexander Wendt en 1987. Los principios fundamentales de la misma son, en palabras de Wendt (1999): “1) que las estructuras de la asociación humana están determinadas principalmente por ideas compartidas más que por fuerzas materiales; y 2) que las identidades y los intereses de los actores intencionales están construidos por esas ideas compartidas en lugar de estar dados de manera natural”. Este autor entiende a su vez que en esta teoría impera un carácter institucionalista, que posibilitaría el orden en las relaciones internacionales.

Sin embargo, cabe mencionar que, como afirma Vitelli (2014), aún existe cierta renuencia por parte de muchos autores, a la hora de identificar al constructivismo como teoría completamente formada o válida. A los efectos de este trabajo monográfico, se utilizará el enfoque constructivista como paradigma o teoría de las relaciones internacionales, obviando los cuestionamientos de la validez teórica y centrándose en lo que esta puede aportarle a la investigación.

Retomando los dos principios centrales del constructivismo de Wendt planteados anteriormente, las asociaciones se dan por ideas compartidas y los intereses de los actores parten de esas mismas ideas. La formación de las asociaciones o estructuras sociales y los agentes en las relaciones internacionales son los asuntos principales sobre los que se ocupa esta teoría. Vinculando esta noción a la temática planteada aquí, la preocupación sobre la ciberseguridad a nivel estatal y luego regional es lo que elevó dicha necesidad a la OEA. Los Estados miembros se asociaron en una primera instancia a dicha organización por intereses e ideas compartidas, y en la actualidad, uno de ellos es la seguridad cibernética.

La noción de instituciones está muy presente en este paradigma, y Salomón ahonda en los tipos de estructuras o instituciones que Wendt desarrolló. Una de ellas es la de seguridad colectiva, un sistema de seguridad con estructura cooperativa, donde los Estados entienden la seguridad de cada uno de ellos como propia. Luego identifica la autotutela como el otro extremo del espectro de las instituciones, y como punto intermedio un sistema donde los Estados no dan importancia a cómo la seguridad de todos ellos está conectada pero entienden que cooperando hay mayor ganancia que manteniéndose por separado. Las organizaciones internacionales son para Wendt un

tipo de institución, que a su vez modifican o moldean los intereses de los Estados (Salomón, 2002). Utilizando la Estrategia Interamericana Integral para Combatir las Amenazas a la seguridad cibernética, la OEA plasma ciertos lineamientos y prácticas a seguir por parte de los Estados miembros, y con esto puede llegar a modificar los objetivos de los mismos. El enfoque ya no se encuentra en los intereses nacionales individualizados, sino que hay una meta o deseo mayor, el de la organización buscando el perfeccionamiento de la ciberseguridad a nivel regional.

Volviendo al concepto de seguridad con estructura cooperativa ya planteado, la seguridad de cada uno de los miembros de dicho sistema están profundamente ligadas entre sí. El artículo 3 de la Carta afirma que "la agresión a un Estado americano constituye una agresión a todos los demás Estados americanos". Se trata entonces de una estructura de seguridad cooperativa, donde cada Estado es responsable de la seguridad del resto, y viceversa. Dentro de la perspectiva de la OEA, la seguridad conforma un principio compartido por los Estados miembros.

Capítulo II

Ciberseguridad en la región

De acuerdo con el informe conjunto del BID y la OEA sobre ciberseguridad en América Latina y el Caribe (2016), gran parte de los Estados en dichas regiones no han logrado aún la capacidad para contrarrestar las amenazas que supone el ciberdelito. Mediante un Modelo de Madurez de Capacidad de Seguridad Cibernética, este trabajo analiza a los Estados utilizando 49 indicadores (divididos en cinco dimensiones: políticas y estrategia nacional de seguridad cibernética, cultura cibernética y sociedad, educación, formación y competencias en seguridad cibernética, marco jurídico y reglamentario, y normas, organizaciones y tecnologías), y concluye que muchos de ellos se encuentran vulnerables a ciberataques de gran magnitud; cuatro de cada cinco no cuentan con estrategia de ciberseguridad, y dos de cada tres no posee una unidad de control y comando de ciberseguridad.

El mismo informe sostiene a su vez que existe un esfuerzo de las Américas por desarrollar dichas estrategias y nivel de reacción frente al cibercrimen, por lo que se posiciona como líder global en la materia. Pero a nivel de América Latina y el Caribe, las iniciativas se encuentran poco desarrolladas (OEA, BID, 2016).

José Carlos Hernández (2018), en un artículo de análisis dedicado al estudio de las estrategias nacionales de ciberseguridad que existen hasta la fecha en América Latina, afirma que en dicha región "la mayor parte de los Estados dispone de capacidad de respuesta ante ciberataques, pero lo cierto es que sólo seis han diseñado una Estrategia de Ciberseguridad". Estos son: Colombia, Panamá, Paraguay, Chile, Costa Rica y México.

Gran parte de los Estados de la región no tienen las herramientas necesarias para hacer frente al cibercrimen, que genera pérdidas por alrededor de 90.000 millones de dólares al año en dichos Estados. (OEA, BID, 2016). El riesgo y las pérdidas económicas aumentan en la medida en que dicha región crece en conectividad. Los incidentes cibernéticos son cada vez más frecuentes, y ha obligado a actores privados y públicos a intentar fijar medidas fuertes en seguridad cibernética, y al mismo tiempo cooperar en el intercambio de información.

Se entiende que en América Latina y el Caribe, el trabajo realizado hasta el momento y los esfuerzos por fomentar la ciberseguridad "están en una etapa temprana" y "los principales desafíos que enfrenta la región en seguridad cibernética son el desarrollo de capacidades en todos los países, la mejora de la cooperación en delitos cibernéticos y el intercambio de información sobre mejores prácticas, amenazas y vulnerabilidades". (OEA, BID, 2016)

Se identifica la creación de múltiples CSIRTs en toda la región, que colaboran entre sí y fomentan la comunicación y el intercambio de conocimientos y buenas prácticas. Dichos CSIRTs no cuentan con la misma capacidad de respuesta, y se encuentran en diferentes etapas de desarrollo, por lo que se hacen falta mejoras. El mismo escenario se da con respecto a las herramientas jurídicas que dispone cada Estado frente al ciberdelito. La mayor parte de los Estados le dan una gran importancia a reformar los regímenes legales para hacer efectiva la justicia penal frente a estos delitos.

Sin embargo, en lo referente al aspecto económico, se ha afirmado que “el estado actual de la economía digital en América Latina y el Caribe deja mucho que desear; se caracteriza por un retraso general en calidad, por detrás de otras partes del mundo y con grandes variaciones en la región”. Algo similar sucede con la conectividad, y la cantidad de usuarios de internet en la región. (OEA, BID, 2016). En cuanto a la existencia de estrategias de seguridad cibernética, como se mencionó anteriormente, son pocos los Estados que han logrado llevarla a la práctica. Los organismos específicamente dedicados a la ciberseguridad en dichos Estados aún no cuentan con la organización y coordinación adecuadas entre ellos para lograr cumplir su tarea eficientemente. Frente a esta situación, en general el sector privado ha avanzado más en el tema que los entes gubernamentales.

De forma resumida, se entiende que una estrategia nacional se compone los siguientes elementos: es necesaria la creación de un órgano de coordinación presente en la Presidencia para administrar la gestión y puesta en práctica de las directrices; a su vez, los ministerios deben tener asignadas responsabilidades en ciberseguridad, cuyo accionar debe estar fuertemente vinculado con el sector privado para lograr una alta colaboración en los sectores productivos. La presencia de un CERT nacional y departamento de Policía especializada, y realizar esfuerzos en cooperación regional y global son otros dos elementos claves que deben estar presentes en una estrategia nacional en ciberseguridad (OEA, BID, 2016).

Para mostrar los diferentes niveles de desarrollo en ciberseguridad que existen en la región en cuanto a ciberseguridad, se tomarán dos Estados como ejemplo. El principal criterio utilizado para seleccionar dos Estados y de esta manera mostrar la diversidad de realidades estatales, es la existencia de una Estrategia de Ciberseguridad Nacional. Cumpliendo con dicha condición, este autor considera que un Estado se encuentra mejor posicionado y más avanzado en la temática, ya que reúne una condición fundamental para el eficaz combate del ciberdelito.

Un primer ejemplo es Chile, Estado que cuenta con una Estrategia de Ciberseguridad Nacional detallada en el corto y mediano plazo, conocida como Política Nacional de Ciberseguridad (PNC). Esta define los órganos responsables de la misma, así como el conjunto de medidas a ejecutar para cumplirla, con el año 2022 como plazo. El gobierno y sus instituciones están altamente concientizados sobre la importancia de

la ciberseguridad, y el análisis de los activos y debilidades de la infraestructura nacional es permanente. Tanto a nivel del Ministerio del Interior, como de Presidencia y hasta las Fuerzas Armadas chilenas cumplen un papel de responsabilidad en garantizar la ciberseguridad nacional. En lo referente al orden jurídico, cuenta con el Decreto nº 1299 que define las leyes y autoridades competentes; los delitos cibernéticos están debidamente identificados en la legislación, y los juzgados tienen la habilidad para manipular evidencia electrónica. Por otra parte, el sector privado está aumentando su capacidad para hacer frente a la ciberdelincuencia, y hay una amplia oferta de múltiples cursos y capacitaciones (Hernández, 2018).

La PNC incluye como medida a implementar la creación de una Política de Ciberdefensa, la cual establece lo siguiente:

> "El Estado de Chile considera que un ciberataque puede llegar a ser tan dañino como un ataque armado. Chile podrá considerar los ciberataques masivos sobre su soberanía, sus habitantes, su infraestructura, o aquellos que afecten gravemente sus intereses, como un ataque armado, y de acuerdo con el artículo 51 de la Carta de las Naciones Unidas, podrá hacer uso de los medios que estime apropiados, tanto físicos como digitales, en el ejercicio de su derecho a la legítima defensa" (Diario Oficial de la República de Chile, 2018)

Esto denota una marcada intención del gobierno chileno de considerar el ciberespacio y los activos estatales como parte del "territorio" nacional a defender, e igual de importantes que cualquier otro elemento de su soberanía. Chile cuenta a su vez con su propio CSIRT.

Chile se ha enfrentado en el último tiempo a ciberataques de gran magnitud que perjudicaron tanto a los ciudadanos como a entidades bancarias. En junio del 2018, una filtración masiva de datos bancarios de miles de clientes nacionales chilenos constituyó una de varias situaciones similares en el país andino. Otro episodio a comienzos de dicho año significó la pérdida de diez millones de dólares para el Banco de Chile (Emol, 29 de agosto de 2018). Estos sucesos pusieron en evidencia ciertas fallas de este Estado

para hacer frente al ciberdelito en la práctica, y una necesidad de implementar nuevas herramientas para la protección de sus ciudadanos.

Frente a estos acontecimientos, en octubre de 2018 el Presidente Sebastián Piñera aprueba un proyecto de ley de delitos Informáticos que busca actualizar la legislación existente en la materia, y anuncia un Instructivo Presidencial de Ciberseguridad estatal. Este documento tiene como objetivo fijar obligaciones a cumplir por los servicios públicos estatales, y la designación de un encargado de ciberseguridad de alto nivel en cada uno de estos servicios (Diario 24 Horas, 2018).

Se entiende por todo lo expuesto anteriormente, que Chile se constituye como un Estado con un interés latente por mejorar constantemente sus herramientas para enfrentar las amenazas que supone el ciberespacio. Igualmente, hoy en día ha realizado grandes avances en ciberseguridad, y su grado de desarrollo en la materia supera en cierto grado el de muchos Estados latinoamericanos, considerando que es de los pocos de la región en contar con una Estrategia Nacional de Ciberseguridad.

El segundo caso regional que se utilizará en el presente trabajo para ejemplificar la diversidad de grados de desarrollo en ciberseguridad es Brasil. De acuerdo con el Índice Global de Ciberseguridad elaborado por la UIT en 2017, Brasil es el tercer país latinoamericano (detrás de México y Uruguay) con un mayor nivel de compromiso en la materia (UIT, 2017). Este Estado cuenta con una estructura descentralizada en cuanto a ciberseguridad, y cuyos principales actores son el Gabinete de Seguridad Institucional de la Presidencia de la República, y el Centro de Defensa Cibernética, vinculado a las Fuerzas Armadas, y la Defensa. No hay un órgano que coordine la implementación de la política de ciberseguridad, y las competencias y responsabilidades se dividen entre los diferentes actores. La falta de un ente coordinador de los esfuerzos es lo que denota la falta de una Estrategia Nacional de Ciberseguridad propiamente dicha. La política de defensa de Brasil o END, aprobada en 2008 y modificada en 2012, incluye el ciberespacio como punto estratégico nacional y nombra al Ejército como líder de la defensa cibernética. La ciberseguridad se incluye entonces como un ámbito más en la política de defensa. Se agrega en el 2012 el CERT como parte de la política de protección cibernética, y existen también varios CSIRTs tanto públicos como privados (OEA, BID, 2016). Por otra parte, el principal organismo investigador de ciberdelitos es la Oficina para la Represión de la Delincuencia Cibernética de la Policía Federal.

Brasil cuenta con un Decreto que dicta una política de seguridad de la información para los organismos públicos, y a partir del 2012, con una Política Cibernética de Defensa aprobada por el Ministerio de Defensa. Gran parte de los documentos dedicados a la ciberseguridad brasileña están bajo la supervisión del Ministerio de Defensa, y también del Ejército brasileño. Este hecho ha generado críticas, ya que se ve este ámbito como ampliamente militarizado (Cruz, 2017). Por otra parte, en el 2014 se sanciona el Marco Civil de Internet, que regula todo lo referente al uso de Internet en Brasil, los derechos, obligaciones y garantías de los usuarios y el accionar del Estado. Esta norma fue cuestionada en cuanto su aplicación, y tachada de inconstitucional por algunos sectores, ya que garantiza ciertos derechos civiles mientras que trastoca otros. A pesar de estas preocupaciones, se lo considera un "documento de avanzada que protege los intereses de los ciudadanos" (OEA, BID, 2016). A su vez, este Estado dispone grandes volúmenes de inversión en las tecnologías de la información.

Por todo lo expuesto anteriormente, es posible afirmar que Brasil cuenta con herramientas jurídicas y organismos con capacidad de respuesta frente al ciberdelito, lo que genera un nivel de ciberseguridad correcto y considerado entre los primeros puestos a nivel regional. Como principal debilidad, se identifica la falta de coordinación entre los organismos involucrados, y un marco que regule dicha relación. Este Estado se encuentra trabajando en estos puntos, pero de momento, no es posible identificar una Estrategia Nacional de Ciberseguridad que impulse el grado de desarrollo brasileño en la materia.

Como es posible observar mediante los ejemplos utilizados y los distintos informes disponibles sobre la realidad regional en ciberseguridad, hay un panorama diverso en cuanto a nivel de desarrollo si se observa cada Estado de la región. Si bien varios Estados tienen un nivel aceptable y cuentan con un grado considerable de compromiso frente a la ciberseguridad, en rasgos generales y comparando con otras regiones, Latinoamérica tiene aún mucho por mejorar. De acuerdo con el informe de la OEA y el BID del 2016, la región es "altamente vulnerable a ciberataques potencialmente devastadores".

Capítulo III

La OEA y su Estrategia Interamericana Integral para Combatir las Amenazas a la seguridad cibernética, y su vinculación con Uruguay

Este documento, aprobado por la Asamblea General de la OEA en el 2004, tiene como principal objetivo la "creación de una cultura de seguridad cibernética" (OEA, 2004). El enfoque de esta resolución es multidimensional y multidisciplinario, para lograr así un entorno regional seguro en cuanto a sistemas de información y vigilancia cibernética. Entre sus metas se encuentra promover una red interamericana de vigilancia mediante la instalación de equipos o grupos de vigilancia y alerta, a nivel nacional. Esto es, los llamados CSIRT mencionados anteriormente.

La Resolución asigna al Consejo Permanente de la OEA (mediante la Comisión de Seguridad Hemisférica) la tarea de unir los esfuerzos de implementación de la Estrategia, que son protagonizados por el Comité Interamericano contra el Terrorismo (CICTE), la Comisión Interamericana de Telecomunicaciones (CITEL) y el Grupo de Expertos Gubernamentales en Materia de Delito Cibernético de la Reunión de Ministros de Justicia o de Ministros o Procuradores Generales de las Américas (REMJA), y otros organismos pertenecientes a la OEA.

Para fomentar la cultura de seguridad cibernética deseada por la OEA, la Resolución establece que el camino para lograrlo será "por medio de las acciones de los Estados Miembros y las iniciativas que emprenderán el CICTE, la CITEL, y el Grupo de Expertos Gubernamentales en Materia de Delito Cibernético de la REMJA" (OEA, 2004). Esta noción de organizaciones internacionales como actores de importancia y gestantes de proyectos comunes permite observar características de la teoría de la interdependencia compleja, la cual las sitúa como protagonistas del escenario internacional, en conjunto con los Estados.

El CICTE tiene como objetivo combatir el terrorismo, principalmente mediante la cooperación entre los Estados miembros, quienes forman parte de dicho Comité y se reúnen de forma anual. Cuenta con 10 programas de temáticas diversas divididos en áreas, entre los que se encuentra la Seguridad Cibernética, contenida en el área de Protección de Infraestructura Crítica. Por su parte, la CITEL cumple el rol de foro

regional de telecomunicaciones, que reúne a gobiernos y el sector privado para promover la Sociedad Global de la Información. Busca proporcionar herramientas y promover el progreso regional de las telecomunicaciones (OEA, 2008).

Por último, las REMJA o Reuniones de Ministros de Justicia u Otros Ministros, Procuradores o Fiscales Generales de las Américas pertenecen al Departamento de Cooperación Jurídica de la OEA, y componen el más importante foro político y técnico en el hemisferio, en materia de cooperación jurídica y justicia internacional (OEA, 2018).

A los efectos de analizar la implementación de esta Estrategia Integral en el ámbito nacional, se desglosará la misma de acuerdo a lo que propone cada uno de los organismos mencionados (CICTE, CITEL y REMJA) y cómo estas iniciativas se vieron reflejadas en Uruguay.

En primer lugar, el CICTE propone la creación de una Red Interamericana de Vigilancia y Alerta, que pretende informar sobre todo lo relativo a la ciberseguridad y brindar respuesta a los incidentes, mediante el apoyo técnico. Esta Red Interamericana será una "red hemisférica que funcione 24 horas al día, 7 días a la semana, de Equipos de Respuesta a Incidentes de Seguridad en Computadoras (CSIRT)" (OEA, 2004). Estos equipos que integrarán la Red no necesariamente deberán ser CSIRT propiamente dichos, sino puntos de contacto de vigilancia y alerta en cada Estado (futuros CSIRT). Sin embargo, sí deberán compartir los siguientes principios: deberán ser locales y nombrados por sus respectivos gobiernos; sistémicos en cuanto a la reevaluación y distribución constante de información; permanentes en lo referido a la mejora constante del programa y capacitación del personal; responsables en el manejo de la información y por último, basados en disposiciones ya existentes para evitar duplicaciones. Esta red de CSIRTs de cada Estado refleja un grado de cooperación entre estos, con la idea de lograr un objetivo común.

En este escenario, para lograr el objetivo de materializar la Red Interamericana, cada Estado depende del accionar del otro. Se denota la interdependencia entre ellos, que parte de un proyecto liderado por una organización internacional gubernamental. Nuevamente se percibe una interdependencia compleja, como la que plantearon Keohane y Nye.

Las medidas a tomar para crear dicha red de CSIRT serán en primer lugar, la identificación de los mismos, el establecimiento de un modelo de servicio mediante la designación por parte de cada gobierno de sus respectivos centros CSIRT en concordancia con las normas internacionales en la materia, y por último, es fundamental garantizar la seguridad y la confianza entre los centros dado el carácter delicado de la información que intercambiarán. Otra tarea inherente a los CSIRT estatales será generar conciencia a nivel de la sociedad, para que el público sepa cómo reportar un incidente cibernético. Por último, los Estados Miembros podrán extender la red hemisférica para asistir a otros Estados en la elaboración de proyectos y planes de ciberseguridad; por otra parte, el Grupo de Practicantes Gubernamentales en Materia de Seguridad Cibernética mantendrá reuniones periódicas para mantener en funcionamiento la red.

La propuesta del CICTE se ve reflejada en Uruguay con la creación del CERTuy en el año 2008 por medio de la Ley 18362. Este Centro lleva a cabo la función de punto de vigilancia y protección de los sistemas estatales. A su vez, es posible afirmar que cumple con los requisitos establecidos en la Estrategia de la OEA. En primer lugar, fue creado mediante ley por el gobierno uruguayo, por lo tanto cumple con la condición de ser local y nombrado por el gobierno. Por otra parte, el carácter sistémico y permanente en cuanto al flujo de información y mejora se ve plasmado en los continuos esfuerzos de perfeccionamiento del sistema que lleva adelante el gobierno en conjunto con la AGESIC y el CERTuy.

El Plan de Gobierno Digital 2020 es un claro ejemplo de esto, ya que agrupa una serie de iniciativas que tienen como objetivo la transformación digital del gobierno, de una manera integral. Se basa en seis áreas de acción con sus respectivos objetivos, entre las que se encuentra el gobierno digital confiable. Los objetivos a lograr por dicha área son: fortalecer el ecosistema de ciberseguridad, promover la gestión de riesgos y continuidad operativa, universalizar la identificación electrónica y por último, adecuar y actualizar el marco normativo para acompasar el desarrollo del Gobierno Digital (AGESIC, 2017).

Para fortalecer el ecosistema de ciberseguridad, en dicho Plan de Gobierno se plantea la creación del Centro Nacional de Operación de Seguridad o SOC nacional. Dicho organismo, mediante la cooperación público-privada, busca detectar y también prevenir incidentes, al tiempo que llevará adelante una función de investigación en

materia de ciberseguridad. Junto con el CERTuy, es uno de los encargados de mantener el flujo de información relevante al ámbito de la ciberseguridad para beneficiar a todos los actores involucrados, y mejorar constantemente la capacidad operativa del gobierno frente a las amenazas cibernéticas. (AGESIC, 2017)

Continuando con lo establecido en la Estrategia de la OEA, la condición de los CSIRT o CERT de ser responsables en el manejo de la información también es uno de los puntos clave en la política de Gobierno Digital, particularmente en la Unidad de Gestión de Incidentes, iniciativa llevada adelante por la AGESIC y conformada por el CERTuy y el SOC. La protección de los activos de información del Estado y prevención de que dicha información pueda ser robada o mal utilizada son sus principales objetivos.

Infograma del Plan de Gobierno Digital de Uruguay, publicado en el 2018 por la AGESIC. Se detalla las seis áreas de acción que lo conforman, y los objetivos de cada área. Extraído de file:///C:/Users/TODOS%20!!!!!/Desktop/plan_de_gobierno_digital.pdf

Siguiendo con las propuestas establecidas en la Estrategia Interamericana Integral de Seguridad Cibernética, la CITEL enfoca sus esfuerzos en el intercambio de información entre los Estados Miembros para generar redes más seguras, y por otra parte, la formulación de normas técnicas para lograr dicho cometido mediante las alianzas público privadas y la cooperación entre Estados. De esta forma, la ciberseguridad entre los Estados está íntimamente ligada entre sí, y se manifiesta un alto nivel de interdependencia. Estos serán asesorados por la CITEL, para que adopten políticas y así impulsar a los proveedores de redes a aplicar normas técnicas de seguridad. Para lograr su objetivo, la CITEL unió esfuerzos con otras organizaciones, como la Unión Internacional de Telecomunicaciones (UIT). Mediante un taller conjunto dedicado a la seguridad cibernética, se adoptó la Resolución CCP.I/RES.49 (IV-04) "Seguridad Cibernética" durante la IV Reunión del Comité Consultivo Permanente I del año 2004. En dicha Resolución se plasma la contribución de la CITEL a la Estrategia Interamericana Integral de la OEA. Este organismo realiza una evaluación de las normas técnicas existentes para luego analizar su posible aplicación en la región americana, poniendo especial énfasis en la necesidad de cooperación e intercambio de información entre los Estados miembros y organismos para lograrlo. Se aclara que la aplicación y desarrollo de dichas normas no será un proceso de iguales características para todos los Estados, ya que el grado de desarrollo nacional en seguridad cibernética tiende a variar dependiendo del Estado miembro.

Si bien en primera instancia la CITEL considera fundamental trabajar en las políticas públicas en telecomunicaciones de cada Estado, el trabajo conjunto del sector público y privado llevará a la adopción de normas técnicas que fomentarán la seguridad de las redes.

Este organismo elaboró un Plan Estratégico 2018-2022, en el cual se fijó metas estratégicas. Entre ellas, se enumera promover la inclusión digital mediante "infraestructuras y servicios digitales seguros y confiables" (CITEL/RES. 79 [VII-18], 2018). Dentro de la estructura organizativa de la CITEL se encuentra el CCP I o Comité Consultivo Permanente I, órgano asesor en telecomunicaciones y las políticas y normativas relacionadas que implementen los Estados. Una de las actividades propuestas en el Plan Estratégico de la CITEL es la de "fomentar el intercambio de mejores prácticas en materia de seguridad en los servicios de telecomunicaciones/TIC y dispositivos, así como el fortalecimiento de las acciones en materia de ciberseguridad",

la cual será llevada a cabo por el CCP I. Uno de los medios que se eligió para lograr esto fue por medio de capacitaciones.

Una de ellas se realizó durante el 2017 en Perú, donde se impartió el "Curso de seguridad de la información y Normas ISO 27001 y 27002", patrocinado por la OEA y la CITEL, en el cual se otorgaron 54 becas a varios Estados miembros de la OEA para que ciudadanos y profesionales vinculados a las Tecnologías de la Información puedan entender y desarrollar un Sistema de Gestión de Seguridad de la Información. Cabe mencionar que Uruguay, por medio de la Agencia Uruguay de Cooperación Internacional (AUCI), solo tuvo un beneficiario de dicho curso.

A su vez, el CCP I se compone de diferentes Grupos de Trabajo, integrados por Relatorías, entre las que se encuentra la Relatoría sobre Ciberseguridad y Evaluación de la Vulnerabilidad. Ha implementado diversos instrumentos al servicio de la región en materia de telecomunicaciones. La Red de Intercambio de Información de las Américas (AISN) es establecida por el CCP. I para ampliar el acceso a Internet en la región, coordinar la aplicación de normas y compartir información relevante.

Otro de los medios para intercambiar información entre los Estados miembros, y promover mejores prácticas y normas técnicas en materia de ciberseguridad son los foros y reuniones. El 26 de setiembre del 2017 se llevó a cabo en Montevideo el Foro de Ciberseguridad de las Américas, organizado por la AGESIC, la Presidencia de la República, el BID y la OEA. En dicho encuentro, se discutió sobre la actualidad en ciberseguridad, estrategias regionales y normativa. El principal propósito fue el intercambio de ideas, y una mirada técnico jurídica en la materia. De acuerdo con el diario El País (2017), por medio de este Foro los países miembros de la OEA expresaron su interés por consolidar y unificar sus políticas en el tema, y establecer un frente común de respuesta regional ante incidentes cibernéticos. Así lo afirmó el gerente del Programa de Ciberseguridad de la OEA Belisario Contreras (El País, 2017). Este evento, organizado en Uruguay por sus organismos estatales, demuestra el interés del gobierno uruguayo en fomentar la cooperación y avanzar en la protección de los activos informáticos estatales.

Si se observan los esfuerzos internos de dicho gobierno para lograr este cometido, cabe mencionar diversos cursos ofrecidos por organismos públicos. El Curso en Ciberdefensa y Ciberseguridad, impartido por la Escuela de Altos Estudios

Nacionales en conjunto con el Ministerio de Defensa, está dirigido tanto a profesionales del ámbito estatal como privado. Esta Escuela tiene como misión contribuir a la implementación de una cultura de estrategia nacional. Por otra parte, desde el año 2009 AGESIC ha ofrecido ciclos de charlas anuales sobre seguridad informática, con participación público-privada, tanto nacional como internacional. El objetivo de estas charlas es generar capacidad de respuesta, promover buenas prácticas y técnicas de seguridad cibernética.

El enfoque de la CITEL se puede vincular también con una necesidad de elaborar normas para la colaboración en ciberseguridad, y mejorar así la capacidad de respuesta coordinada entre los actores (tanto entre los Estados entre sí, como a la interna de estos) frente a incidentes. Como manifiesta el informe "Ciberseguridad: ¿estamos preparados en América Latina y el Caribe?", la ciberseguridad "es un área que está madura para la cooperación regional, si no mundial, para coordinar mejor las políticas e identificar las mejores prácticas, un proceso que los países de América Latina y el Caribe están bien posicionados para liderar" (BID, OEA., 2016).

De acuerdo con este mismo informe, el CERTuy se mantiene en contacto con otros CSIRT a nivel regional y organizaciones internacionales al momento de brindar respuesta a incidentes; a su vez, informa y alerta sobre ataques y riesgos potenciales (BID, OEA., 2016). Denota una actitud activa de cooperación e intercambio de información con otros Estados y organizaciones.

La última iniciativa plasmada en la Estrategia de la OEA es la que plantea el REMJA, y se encuentra muy vinculada a la formulada por la CITEL, ya que se centra en los instrumentos normativos y jurídicos necesarios para garantizar la seguridad de las redes. Se apuntará a proteger a la sociedad de los delitos cibernéticos, y al mismo tiempo, fomentar la cooperación internacional en esta temática. Este Grupo de Expertos "proporcionará asistencia técnica a los Estados Miembros para la redacción y promulgación de leyes que tipifiquen el delito cibernético, protejan los sistemas de información y eviten el uso de las computadoras para facilitar actividades delictivas". (OEA, 2004).

Las REMJA son reguladas por el "Documento de Washington" del 2008, aprobado en la REMJA VII. Este conjunto de disposiciones regula todo lo referente a estas Reuniones: denominación, integración, funciones y su funcionamiento. De

acuerdo con dicho Documento, las REMJA se realizan bienalmente, convocadas por la Asamblea General o el Consejo Permanente de la OEA. Su forma de actuar es a través de recomendaciones, y éste es el carácter de los acuerdos a los que se llegan en dichas Reuniones. Para monitorear la aplicación de estas recomendaciones, se crean Grupos de Trabajo. Uno de ellos es el Grupo de Trabajo en Delito Cibernético, que está integrado por expertos gubernamentales dedicados a la investigación y persecución de dicho tipo de delitos en los Estados miembros de la OEA (REMJA, 2012).

De acuerdo con la Estrategia interamericana de la OEA, este Grupo de Expertos se dedicará a asistir en materia técnica a los Estados miembros, capacitando en la formulación de leyes nacionales que promuevan la confianza en los sistemas de información. La manera de lograrlo es a través de normas que califiquen como delito el uso ilícito de redes y equipos informáticos. Por medio de capacitaciones y talleres, intentará que los Estados miembro promulguen normas de carácter penal que prohíban ataques a los sistemas informáticos, leyes procesales referidas al acceso estatal a los datos y pruebas electrónicas que se requieran frente a un delito. Por último, proporcionará instancias de consulta jurídica para respaldar a los gobiernos en la creación, aplicación y actualización de dichas normas.

El Grupo comienza a reunirse en el año 1999, de cuyas reuniones se presenta luego un informe con recomendaciones para los Estados miembros. Durante la tercera reunión en el año 2003, el Grupo recomendó que se identifiquen o se constituyan unidades nacionales dedicadas a investigar y perseguir la criminalidad cibernética. Por otra parte, los sistemas jurídicos deben poder aplicarse a los delitos cibernéticos, con la correcta tipificación de los mismos, al tiempo que se deben asegurar medidas procesales que permitan obtener indicios o pruebas electrónicas. Por último, instaron a los gobiernos a vincularse a la “Red de Emergencia de 24 horas/7 días”. Esta red para Delitos de Alta Tecnología establecida por el G8 para la conservación de información busca reunir puntos de contacto entre las autoridades de los Estados miembros, que faciliten la obtención de material probatorio electrónico de urgencia. A modo de resumen, las autoridades judiciales de un Estado que necesiten asistencia de otro Estado pueden contactar el punto de contacto nacional de dicha Red, que deberá ponerse en contacto con su homólogo del Estado del cual se requiere la prueba o evidencia (OEA, 2007).

A su vez, en la cuarta reunión llevada a cabo en el 2006, se resaltan los buenos resultados de los talleres dedicados a capacitar en la elaboración de leyes específicas aplicables a delitos cibernéticos que fueron realizados en el 2004 y 2005 e impulsa a los Estados a continuar adecuando sus leyes de combate al crimen cibernético. Por otra parte, insta a los Estados a mejorar la cooperación mutua en este sentido, y la implementación de la Red de Emergencia. Finalmente, hace hincapié en la cooperación público privada para hacer frente a los delitos de este tipo. Para esto, impulsa la creación de una guía de mejores prácticas para así enriquecer la relación entre los organismos encargados de perseguir estos delitos y las empresas proveedoras de internet. Es en esta reunión en la que se plantea a los Estados miembros que consideren poner en práctica los principios emanados del Convenio sobre Ciberdelincuencia, del Consejo de Europa realizado en Budapest en el año 2001.

Continuando con las recomendaciones del Grupo de Expertos en Delito Cibernético, las siguientes a destacar son la séptima reunión del 2012, y la novena que fue realizada en el 2016. En la primera, la recomendación a enfatizar es la que incentiva a las unidades nacionales investigadoras de delitos cibernéticos a desarrollar y mantener páginas web que brinden información a los ciudadanos sobre cómo detectar estas transgresiones y así prevenirlas. Por otra parte en la novena reunión se recomienda a los Estados, entre otras medidas, a fijar medidas para obtener estadísticas sistematizadas anuales sobre las investigaciones y sanciones a estos delitos, y luego se recopilen dichas estadísticas para así informar a la Secretaría Técnica de las REMJA.

Luego de planteadas las recomendaciones del Grupo de Expertos en Delito Cibernético de las REMJA, es necesario analizar el efecto de las mismas en Uruguay y su grado de aplicación. En lo referente a la existencia de leyes que tipifiquen el delito cibernético, no existe en la actualidad legislación específica uruguaya que defina ni regule todo lo relativo a los delitos informáticos. En el año 2014 se presentó un proyecto de ley originado en la Cámara de Senadores, que buscó reglar los delitos informáticos, pero que finalmente fue archivado. En dicho proyecto, se afirma lo siguiente:

> Se tipifican con precisión algunas conductas marcadamente lesivas de bienes jurídicos cuya vulnerabilidad de grado mayor siempre ha estado en la

> mira del Derecho Penal (la fe pública, los derechos fundamentales, entre otros), pero que al ser ejecutadas contra, o por medio de un sistema informático, hoy día requieren de renovadas previsiones legales. (Uruguay, Proyecto de Ley 103462, 2014)

Este proyecto define varios conceptos fundamentales relevantes para la temática, tipifica los que considera delitos informáticos y las penas correspondientes, para luego enumerar los agravantes. Se trató de un claro intento de mejorar la actual respuesta nacional frente a este fenómeno, y darle respaldo jurídico. La clasificación de los delitos fue elaborada de manera multidisciplinaria, ya que intervino el Ministerio del Interior, el Ministerio de Educación y Cultura, la Fiscalía de Corte junto con la AGESIC. Sin embargo, la falta de promulgación de esta ley que quedó en carácter de mero proyecto implica un vacío legal que genera inconvenientes a la hora de enfrentar la ciberdelincuencia. Se afirma entonces que las recomendaciones del Grupo de Trabajo del REMJA en este sentido no se han llevado a la práctica hasta la fecha a nivel nacional.

Otro proyecto de ley fue presentado en el año 2017 durante el Simposio en Ciberseguridad para la Región de las Américas, organizado por la OEA y AGESIC. Dicha ley busca imponer una política penal específica en ciberdelito, intentando hacer propios los principios expresados en el Convenio sobre Ciberdelincuencia de 2001 realizado en Budapest. Se trata de un primer intento por implementar los lineamientos de dicho Convenio entrado en vigor en 2004, que a su vez abriría las puertas para una futura adhesión al mismo por parte de Uruguay. Como establece el informe sobre dicha Convención elaborado por la Asociación por los Derechos Civiles o ADC (2018), el mismo es hasta el momento “el único instrumento internacional que aborda de manera específica el tema de cibercrimen. Si bien el tratado fue creado en el seno de una institución europea, está abierto para que otros estados puedan adherirse”. En la actualidad, de los 56 Estados que forman parte de dicho Convenio, solo cuatro pertenecen a América Latina: Chile, Costa Rica, Panamá y República Dominicana (ADC, 2018).

Es necesario señalar que el Departamento de Cooperación Jurídica de la OEA realiza en su página web una recopilación de la legislación existente por Estado

miembro, que esté relacionada con las recomendaciones de las REMJA y el Grupo de Trabajo de Delito Cibernético. Las leyes mencionadas en el caso de Uruguay son meramente relativas a delitos que se realizan a través de medios electrónicos, y derechos de los ciudadanos pero ninguna específica sobre delitos cibernéticos, ya que como se mencionó anteriormente, en la actualidad no ha sido sancionado ningún instrumento jurídico que regule estos fenómenos. Como disposición relacionada a la temática se menciona únicamente la ley 17.815 sobre violencia sexual, comercial o no comercial cometida contra niños, adolescentes o incapaces. Dicha ley trata sobre la fabricación, comercialización y difusión de pornografía con imágenes de menores o incapaces.

Siguiendo con las recomendaciones y su aplicación a nivel nacional, la creación de unidades dedicadas a investigar y perseguir estos delitos se ve reflejada en el contexto nacional en diferentes instancias. En primer lugar, mediante el Decreto N°254/003 del año 2003, que crea la División de Delitos Informáticos, que se encuentra dentro del Departamento de Delitos Complejos de la Policía de Montevideo. De acuerdo con María José Viega y Federico Carnikian (2010), esta División se creó de manera urgente, es decir, para hacer frente al auge de todo tipo de ilícitos que podían considerarse delitos informáticos ya que se perpetuaban a través de Internet, pero para los cuales no existía tratamiento o unidad especializada en ellos. Otra aplicación de esta recomendación de las REMJA es la creación del CERTuy, ya que este organismo creado en el 2008 tiene como principal función proveer soluciones a los incidentes informáticos, realizar alertas sobre posibles amenazas e investigar y asesorar en la mejora de la seguridad informática.

Como tercera unidad especializada en seguridad cibernética y la detección de ataques, se identifica el Centro de Operaciones de Seguridad (SOC), mencionado anteriormente. Este Centro se dedica a analizar fuentes de datos tanto públicas como privadas, con el objetivo de prevenir, detectar, analizar y dar respuesta a incidentes de ciberseguridad. (AGESIC, 2017) Por más que pertenezca al ámbito estatal, busca ser un referente de buenas prácticas y promover la cooperación entre los diferentes sectores involucrados. Es también uno de sus objetivos el alcanzar capacidad operativa para detectar ataques cibernéticos de manera ininterrumpida, es decir, en cualquier horario y los 365 días del año. Se podría aproximar que a través del SOC las sugerencias del Grupo de Trabajo de las REMJA relativas a la capacidad de respuesta 24 horas, 7 días a la semana tuvieron cierta aplicación práctica a nivel nacional, pero no específicamente

en el sentido de Uruguay vinculándose oficialmente a la “Red 24/7” establecida por el G8. Hasta la fecha, Uruguay no se ha integrado a la misma.

El SOC cumple en rasgos generales las recomendaciones del Grupo de Trabajo de Delito Cibernético, en la medida en que intenta propiciar una red de emergencia, impulsa la cooperación público privada, hace hincapié y busca ser referente en las buenas prácticas de seguridad informática, y brinda respuesta e investiga sobre los incidentes en dicha materia.

El objetivo del SOC se ve plasmado en la Agenda Uruguay Digital, un documento de AGESIC que nuclea las iniciativas gubernamentales para el desarrollo de las tecnologías de la información. El objetivo 41 de dicha Agenda es “articular las acciones de las múltiples partes interesadas y potenciar su cooperación mediante un Centro Nacional de Operación de Ciberseguridad (SOC Nac) con la participación público-privada”. (AGESIC, 2017)

En cuanto a la recomendación de las REMJA de publicar puntos de contacto para formar eventualmente una Red de Emergencia, se puede observar que en la página web del Departamento de Cooperación Jurídica de la OEA se encuentra publicado un directorio con los puntos de contacto de delito cibernético por Estado miembro de la OEA, y en el caso de Uruguay, menciona únicamente al Departamento de Crimen Organizado, perteneciente a la Dirección Nacional de Información e Inteligencia; y como segundo punto de contacto, al Comisario-Jefe del Departamento de Delitos Complejos. (OEA, 2014)

Siguiendo con la misma propuesta por parte de las REMJA, se puede afirmar que tanto la División de Delitos Informáticos como el CERTuy tienen páginas web que proporcionan información a la población sobre los tipos de incidentes y las maneras de detectarlos. En dichas páginas también es posible obtener información estadística sobre dichos delitos y su incidencia en el contexto nacional. Se puede comprobar entonces que las recomendaciones del Grupo de Trabajo se han puesto en práctica.

Finalmente, el planteo de implementar una guía de buenas prácticas se ve aplicado tanto en los objetivos generales del SOC, así como también por medio de talleres para los Estados miembros de la OEA. Específicamente en julio del 2012 se llevó a cabo en Montevideo el Taller Regional sobre Buenas Prácticas en Seguridad y Crimen Cibernético, organizado por la AGESIC en conjunto con el CERTuy, la Secretaría del CICTE y el Grupo de Trabajo en Delito Cibernético de las REMJA.

(AGESIC, 2012) Este Taller reunió a expertos y autoridades en seguridad y crimen cibernético, junto con los usuarios pertenecientes a los CSIRTs. El hecho de que la organización partiera de dos organismos nacionales y se realizara en Uruguay denota el interés y empeño a nivel gubernamental por involucrarse en iniciativas que posibiliten mejorar la ciberseguridad a nivel regional y promover las buenas prácticas en la materia.

Capítulo IV

Uruguay y su plan de acción en ciberseguridad

En primer lugar, es necesario proporcionar el marco jurídico que se ha generado a nivel nacional en materia de ciberseguridad, para luego entender sus repercusiones prácticas. Si bien existen leyes y decretos previos vinculados a la temática de las redes de información y cómo estas son utilizadas por los organismos estatales, las disposiciones fundamentales que constituyen el marco jurídico de ciberseguridad de Uruguay son las que se detallan a continuación.

La ley 17.930 del año 2005 dedicada al presupuesto nacional, crea mediante el artículo 72 la Agencia para el Desarrollo del Gobierno Electrónico, cuyo objetivo es “la mejora de los servicios del ciudadano, utilizando las posibilidades que brindan las tecnologías de la información y las comunicaciones” (Ley N°17930, 2005). Este organismo, con autonomía técnica, será denominado Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información al año siguiente, mediante el artículo 54 de la ley 18.046 que sustituye al de la ley mencionada anteriormente, para luego convertirse en la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento o AGESIC por medio de la ley 18.172 de ese mismo año. Esta ley agrega que la misión de dicha Agencia es promover la sociedad de la información y el conocimiento, para que tanto los individuos como las empresas y el Gobierno utilicen las redes de comunicación de la mejor forma posible. Para lograr este cometido, es necesario impulsar la seguridad de dichas redes para hacerlas confiables. Se le asigna como función “concebir y desarrollar una política nacional en temas de seguridad de la información, que permitan la prevención, detección y respuesta frente a incidentes que puedan afectar los activos críticos del país” (Ley N°18172, 2006).

Por lo expuesto, se entiende que el Estado toma como propia la tarea de establecer una política de seguridad informática, lo que la convierte en una política pública. Crea organismos que emanan del tronco de la administración pública para que se encarguen de esta misión, y les designa capacidad de acción dentro del ámbito de la ciberseguridad. La Ley 18.362, en su artículo 74, dota a AGESIC de la facultad de apercibir a los organismos que no cumplan con la normativa vigente aplicable a las tecnologías de la información (Ley N° 18362, 2008). Esto implica que es imperativo para la administración pública y sus múltiples organismos cumplir con las directivas de la AGESIC y que, de no hacerlo, pueden ser penalizados legalmente.

Entre los decretos dedicados al ámbito de la ciberseguridad, es posible identificar el Decreto 452/009, del 28 de setiembre de 2009 destinado a brindar confianza a los sistemas y activos de información que manejan los organismos públicos mediante la gestión adecuada de la seguridad, decretó la obligación de que tanto las Unidades Ejecutoras (del Inciso 2 al 15 del Presupuesto Nacional) como los Gobiernos Departamentales, Entes Autónomos y demás adopten una Política de Seguridad de la Información basada en la "Política de Seguridad de la Información para Organismos de la Administración Pública".

Dicha Política fue incorporada al Decreto en los Anexos, y se propone evitar la "destrucción, divulgación, modificación y utilización no autorizada de toda información, comprometiéndose a desarrollar, implantar, mantener y mejorar continuamente un Sistema de Gestión de Seguridad de la Información" (Decreto N°452/009, 2009). La Seguridad tiene como principales fundamentos la protección de la confidencialidad, la integridad y la disponibilidad de la información. Para lograrlo, se deben implementar una serie de medidas de control, que serán llevadas a cabo por el Responsable de la Seguridad de la Información, designado por el Organismo. De acuerdo con presente Decreto, cada Organismo debe fijar objetivos anuales para la Seguridad de la Información, monitorear los posibles riesgos de la misma e implementar acciones de prevención y gestión de incidentes. A su vez, es obligación brindar capacitación y concientizar en seguridad a todo el personal.

Otro Decreto relevante es el Decreto 450/009, que aprueba los Principios y Líneas Estratégicas para el Gobierno en Red, elaborados por AGESIC en el 2009. Dada la política pública de Gobierno Electrónico llevada adelante en los últimos años, era

necesario fijar los postulados y lineamientos con los que se encuadren las acciones de dicha política. Los principios se componen del conjunto de valores con los que medir el nivel de desempeño de los planes que se propongan, mientras que los lineamientos dictan la forma en que se llevarán dichos planes a cabo. Es tarea de AGESIC la de difundir los principios y lineamientos, y a su vez evaluarlos en su aplicación y fiscalización.

Estos principios evocan la necesidad de brindar un marco estratégico que encauce la mencionada política estatal de Gobierno en Red. La tecnología dedicada a la información y comunicación o TIC es un instrumento fundamental en este contexto, y así lo demuestran los múltiples usos que le da el Estado. Con esto busca "construir una Administración enfocada en el ciudadano, siempre accesible y más cercana" (Decreto Nº450/009, 2009). Este enfoque está orientado principalmente a optimizar los trámites administrativos de diferentes organismos, para evitar así la repetición innecesaria. El Gobierno en Red demanda una política integral del uso de las TIC, la cual se compone de herramientas que permiten fijar criterios de aplicación de estas tecnologías. Entre dichos parámetros se encuentran los principios y lineamientos, mejores prácticas, entre otros.

Los principios enumerados en el Decreto son, en primer lugar, el de la igualdad en la prestación de servicios para quienes no utilicen medios electrónicos para vincularse con la administración pública, de modo que no exista discriminación ni ningún tipo de restricción. En segundo lugar, la transparencia en los trámites administrativos y servicios públicos utilizando para esto los medios electrónicos; el principio de la accesibilidad de la información y los servicios electrónicos, para que los usuarios accedan a ellos de manera confiable y clara, garantizando el acceso universal para la igualdad de condiciones al ejercer sus derechos. Se enumera también el principio de eficacia y eficiencia, vinculado al uso de estos medios electrónicos para mejorar los servicios de información para los usuarios; el principio de cooperación e integralidad en relación con los vínculos entre los organismos públicos, el principio de confianza y seguridad en los servicios y uso que realice el Estado de la información obtenida por medios electrónicos, y por último, el principio de neutralidad tecnológica referido a la ausencia de una tecnología específica predilecta, sino que se deja libertad para los organismos de vincularse con la sociedad de diversas formas.

En cuanto a los lineamientos, se señalan el foco en el ciudadano para que éste sea el beneficiado por los proyectos, promoción del acceso universal a las TIC, la especialización y el alineamiento estratégico en la concreción de planes y proyectos para lograr los objetivos propuestos por cada organismo. Otras líneas estratégicas que establece el Decreto son: la sustentabilidad y generación de capacidades (financieras, institucionales y de recursos humanos) para mantener los proyectos de Gobierno Electrónico, la seguridad para preservar los activos informáticos y evitar incidentes, la interoperabilidad o el relacionamiento entre organismos estatales mediante el intercambio de información e integración de datos, la optimización de recursos TIC por medio de la colaboración entre instituciones y una correcta gestión de los activos, el apoyo a la industria nacional a través de la alineación de los proyectos, y por último, la innovación en el uso de las TIC para crear valor para los organismos y usuarios. (Decreto N°450/009, 2009).

IV. I: Aplicación del derecho vigente analizado

Retomando la conceptualización del organismo AGESIC que se mencionó anteriormente, entre sus objetivos estratégicos plasmados en su página web se encuentran la promoción de un Gobierno abierto, la integración de las instituciones estatales mediante los medios tecnológicos, facilitar el relacionamiento de la sociedad con el Estado y promover un ecosistema de ciberseguridad, entre otros. Su estructura operativa se divide en diferentes áreas, siendo una de ellas la seguridad de la información, cuyo cometido principal es llevar adelante un marco regulatorio en materia de seguridad de la información para el Gobierno Electrónico y, por otra parte, fiscalizar y vigilar su acatamiento. Dentro del área de Seguridad de la Información de la AGESIC, se distinguen tres divisiones: Identificación Electrónica, Gestión de la Seguridad de la Información, y el Centro Nacional de Respuesta a Incidentes de Seguridad Informática (CERTuy) (AGESIC, 2017).

Un CERT o Computer Emergency Response Team es un equipo de respuesta ante incidentes informáticos y también cumple el rol de centro coordinador. Sin embargo, no siempre este equipo de expertos recibe el nombre de CERT a nivel mundial, ya que es un nombre registrado en Estados Unidos. Debido a esto, los centros

de respuesta nacionales reciben diferentes nombres en otros países; ejemplos de estos casos son los CSIRT (Computer Security Incident Response Team), IRT (Incident Response Team), CIRT (Computer Incident Response Team), entre otros.

El CERTuy fue creado por el artículo 73 de la Ley N° 18362, de octubre de 2008 y está regulado por el Decreto N° 451/009, donde se establece que la Agencia a través de dicho Centro buscará proteger los activos informáticos críticos del Estado y sus sistemas. Sus integrantes son expertos, responsables de la creación de iniciativas en prevención y solución de incidencias de seguridad. Entre sus funciones cardinales se encuentran: el asesoramiento de la administración pública en materia de políticas y vías de acción de seguridad informática, la protección de los sistemas informáticos claves para el Estado, proveer soluciones a incidentes de seguridad informática en instituciones estatales, proponer normas que amplíen la seguridad y coordinar esfuerzos con otros responsables estatales en seguridad, asesoramiento en la materia y funciones de alerta frente a amenazas, entre otras funciones. (AGESIC, 2017)

A su vez, este Centro forma parte de la iniciativa de Seguridad y Confianza de AGESIC, denominada “Gestión de Incidentes” y llevada adelante por dos equipos: el CERTuy y el Centro de Operaciones de Seguridad (SOC). Éste último busca “mejorar la capacidad operativa en la detección de incidentes de ciberseguridad, partiendo de un enfoque 24x7 on-site, procesamiento y análisis de grandes volúmenes de datos y la colaboración operativa entre el sector público, privado, academia y sociedad civil” (AGESIC, 2017).

Continuando con la normativa nacional vigente en materia de ciberseguridad, el 7 de abril del 2014 se crea el Decreto Nº 92/014, el cual reglamenta el artículo 149 de la ley 18719. Por medio de dicho decreto, se plantean tres directrices que actúan como un nuevo marco de ciberseguridad para los organismos públicos. Estas pautas están vinculadas a los dominios de internet, los correos electrónicos institucionales y los centros de procesamientos de datos de dichos organismos. Mediante la optimización y estandarización del uso de los dominios de internet (gub.uy y mil.uy), efectivizar correos institucionales seguros y garantizar la confidencialidad y disponibilidad de los datos que maneja la Administración Central. Este decreto establece la obligatoriedad de estas medidas, y señala a AGESIC como el organismo encargado de observar su cumplimiento.

Por otra parte en el año 2015, mediante el Decreto N°36/015 se crea el Centro de Respuesta a Incidentes de Seguridad Informática en el Ministerio de Defensa nacional (D-CSIRT), debido a una necesidad percibida, ante la posibilidad de que los incidentes en seguridad informática pudieran afectar la órbita de la seguridad y defensa nacional. Este Centro tiene como rol principal ser el coordinador de las acciones de respuesta y prevención vinculadas a la gestión de incidentes de seguridad informática para las Unidades Ejecutoras y Dependencias del Ministerio, y también colaborar con otras instituciones, de la mano del CERTuy (Decreto N°36/015, 2015). A su vez, debe planificar y ejecutar una política de gestión de riesgos, en concordancia con lo establecido por el CERTuy; asistir en la alerta sobre incidentes y brindar soluciones en materia de seguridad. Mediante la integración de todas las Unidades Ejecutoras y dependencias de dicho Ministerio, se creará un Plan de Trabajo común, para unificar criterios de seguridad de la información y nombrar un Responsable de la Seguridad, siguiendo con lo establecido en el Decreto 452/009. Por último, en el artículo 12 del Decreto dedicado al D-CSIRT, se establece que la gestión de incidentes se realizará "a través de su reporte por medio de las vías disponibles para tal fin, ejecutándose las comunicaciones y operativas correspondientes con los distintos Responsables de Seguridad de la Información designados dentro de la comunidad objetivo". (Decreto N° 36/015, 2015)

Consideraciones finales

A modo de conclusión, luego de haber analizado en forma general el entorno regional y profundizado en la Estrategia de la OEA y sus alcances para Uruguay, es posible realizar determinadas consideraciones sobre el grado de aplicación de la misma y el nivel de ciberseguridad que ha alcanzado Uruguay hasta la fecha, como resultado de dicha influencia y otros aspectos a tener en cuenta.

En primer lugar, queda demostrado que la OEA se encuentra altamente comprometida con la ciberseguridad, y la ubica como un tema fundamental de su agenda, lo que lo convierte a su vez en tema fundamental de las agendas

gubernamentales de sus respectivos Estados miembros. Se manifiestan así los principios de la teoría de la interdependencia compleja, elaborada por Keohane y Nye. Estos autores entienden que los organismos internacionales son tan protagonistas como los Estados, realizan proyectos a nivel internacional y pueden influenciar las agendas de estos. La ciberseguridad de cada Estado se externaliza y se conecta con la de los demás, convirtiéndose en una red interdependiente. A su vez, el hecho de que los Estados compartan información y cooperen entre sí fomenta la apertura entre ellos, lo que aumenta la dependencia (que de acuerdo con la teoría que está siendo manejada, es proporcional a la apertura).

Se puede afirmar que Uruguay cuenta con ciertos proyectos jurídicos potenciales para lidiar con la ciberdelincuencia, que en opinión personal, deberían tomar mayor importancia y promulgarse lo antes posible. Esto generaría conciencia en la sociedad, al tiempo que posibilitaría herramientas para el combate de estos delitos mediante sanciones. Por otra parte, también tiene organismos dedicados específicamente a la ciberseguridad que han probado ser proactivos en la prevención y detección de estos hechos. Hay iniciativas y en muchos casos, se encuentra a la vanguardia a nivel regional.

Luego de haber realizado una descripción en profundidad de la Estrategia en Ciberseguridad de la OEA y las pautas o recomendaciones que fijan cada uno de los organismos que la protagonizan, se realizó el análisis de la influencia de estos sobre Uruguay. A partir de este trabajo, se puede afirmar que Uruguay cumple en mayor o menor medida con las recomendaciones del CICTE, la CITEL y las REMJA, más específicamente del Grupo de Trabajo en Delito Cibernético.

En cuanto a lo que propone el CICTE, Uruguay cumple con la mayor parte de las condiciones para integrar la Red Interamericana de Vigilancia y Alerta. Cuenta con su propio CSIRT (CERTuy), que reúne los requisitos exigidos. A nivel regional, coopera en ciberseguridad, y cuenta además con el SOC como organismo que realiza esfuerzos en el mismo sentido.

Lo que propone la CITEL no se ve reflejado de manera tan clara en el panorama nacional. Uruguay no cuenta con normas técnicas en ciberseguridad, y no tiene una participación importante en los cursos brindados por el organismo en la materia. Aun así, participa activamente y organiza foros para el intercambio de información con otros

Estados, y también entre el sector público y privado. Coopera con la región y se considera como un punto importante en la política uruguaya en ciberseguridad.

Por último, las diferentes reuniones del Grupo de Trabajo de las REMJA llegaron a un número de recomendaciones para los Estados miembros. A nivel general, se puede afirmar que Uruguay aplicó las recomendaciones en gran medida, fundamentalmente en lo que refiere a la creación de unidades especializadas en ciberseguridad, en las guías de buenas prácticas, y en la existencia de páginas web actualizadas que brindan información pertinente sobre el tema tanto a la población como al sector privado y empresas.

Lo que aún no se ha cumplido y se reitera en la Estrategia de la OEA en muchas oportunidades es la creación de legislación específica, que tipifique los delitos cibernéticos. En este punto, Uruguay se encuentra atrasado a nivel global y debe impulsar esta iniciativa para lograr un enfoque más integral de lucha contra la ciberdelincuencia.

Si bien Uruguay no cuenta con su propia Estrategia Nacional de Ciberseguridad, si ha logrado importantes avances a nivel público, ya que los entes gubernamentales están obligados a generar políticas de seguridad cibernética. A su vez, la Política de Defensa Nacional existente menciona medidas en ciberseguridad, y existen campañas a nivel nacional para concientizar a la sociedad. Por lo tanto, a nivel estatal, Uruguay tiene herramientas específicas que buscan aumentar el nivel de protección frente a estos fenómenos. Existe una Unidad especializada en delitos cibernéticos con capacidad forense, y los sectores públicos y privados tienen capacitación constante y se encuentran bien capacitados para enfrentar el panorama actual.

Se puede concluir que, en general, Uruguay tiene un nivel adecuado de ciberseguridad, que cuenta con herramientas con capacidad de respuesta y que en definitiva, ha logrado aplicar gran parte de lo recomendado por la Estrategia Interamericana Integral de Seguridad Cibernética de la OEA. El gran “debe” con respecto a esta, y también hablando de ciberseguridad en general, es la falta de legislación específica que tipifique los delitos ya que genera un peligroso vacío legal. Es fundamental que se solucione lo antes posible para disminuir las posibilidades de que dichos crímenes se lleven a cabo, o bien penalizar los mismos y concientizar a la población sobre los riesgos.

Referencias Bibliográficas

Acurio del Pino, S (s.f). *Delitos Informáticos: Generalidades.* Recuperado de www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

AGESIC (2017). Centro de Operaciones de Seguridad (SOC). Recuperado de https://www.agesic.gub.uy/innovaportal/v/6672/1/agesic/centro-de-operaciones-de-seguridad--soc.html

AGESIC (2017). Centro Nacional de Respuesta a Incidentes de Seguridad Informática (Seguridad de la Información). Recuperado de https://www.agesic.gub.uy/innovaportal/v/2149/1/agesic/centro-nacional-de-respuesta-a-incidentes-de-seguridad-informatica-seguridad-de-la-informacion.html

AGESIC (2017). Foro de Ciberseguridad de las Américas. Recuperado de https://www.agesic.gub.uy/innovaportal/v/6586/1/agesic/foro-de-ciberseguridad-de-las-americas.html

AGESIC (2017). Gestión de Incidentes. Recuperado de https://www.agesic.gub.uy/innovaportal/v/3847/14/agesic/que-es.html?idPadre=3954

AGESIC (2018). *Plan de Gobierno Digital 2020: Transformación con equidad*. Recuperado de file:///C:/Users/TODOS%20!!!!!/Desktop/plan_de_gobierno_digital.pdf

AGESIC (2012). Taller Regional sobre Buenas Prácticas en Seguridad y Crimen Cibernético. Recuperado de https://www.agesic.gub.uy/innovaportal/v/2292/1/agesic/taller-regional-sobre-buenas-practicas-en-seguridad-y-crimen-cibernetico.html

Asociación por los Derechos Civiles (marzo, 2018). La Convención de Cibercrimen de Budapest y América Latina: Breve guía acerca de su impacto en los derechos y garantías de las personas. Volumen 1. Recuperado de https://adcdigital.org.ar/wp-content/uploads/2018/03/Convencion-Budapest-y-America-Latina.pdf

Barrios, M.A. (2009). *Diccionario Latinoamericano de Seguridad y Geopolítica.* Buenos Aires: Biblos.

Carbajal Azcona, J. Definición de ciberseguridad y riesgo (11 de julio de 2017). *Instituto de Economía Digital.* Recuperado de https://www.icemd.com/digital-knowledge/articulos/definicion-ciberseguridad-riesgo/

Centro Latinoamericano de Administración para el Desarrollo (2007). *Carta Iberoamericana de Gobierno Electrónico.* Recuperado de old.clad.org/documentos/declaraciones/cartagobelec.pdf

CERTuy (2016). Ciclo CERTuy de charlas sobre Seguridad Informática. Recuperado de https://docplayer.es/7556036-Ciclo-certuy-de-charlas-sobre-seguridad-informatica.html

CITEL (2018). Cursos de Capacitación. Recuperado de https://www.citel.oas.org/es/Paginas/Training-Courses.aspx

CICTE (2012). Declaración "Fortalecimiento de la Seguridad Cibernética en las Américas". OEA/Ser.L/X.2.12 CICTE/DEC.1/12 rev. 1. Recuperado de https://www.sites.oas.org/cyber/Documents/Declaracion%20del%20Fortalecimiento%20de%20la%20Seguridad%20en%20las%20Americas.pdf

CITEL (s.f). Estructura del CCP.I. Recuperado de https://www.citel.oas.org/es/Paginas/PCCI/Structure.aspx

CITEL (2000). Informe Anual de la Comisión Interamericana de Telecomunicaciones. OEA/Ser.G CP/doc. 3269/00. Recuperado de http://www.summit-americas.org/Informe%20Anual%20de%20CITEL.htm

Comisión de Seguridad Hemisférica, OEA (2009). Fomento de la confianza y la seguridad: Lista de medidas. Recuperado de http://www.oas.org/csh/spanish/mfclist.asp

Departamento de Cooperación Jurídica, OEA (s.f). Reuniones del Grupo de Expertos Gubernamentales sobre Delito Cibernético. Recuperado de http://www.oas.org/juridico/spanish/cybersp_expertos.htm

Díaz, C. En qué está la realidad de Chile en materia de ciberseguridad a un mes de la primera filtración masiva de datos bancarios (29 de agosto de 2018). *Emol*. Recuperado de https://www.emol.com/noticias/Tecnologia/2018/08/29/918792/Ataques-y-filtraciones-Como-esta-Chile-en-materia-de-ciberseguridad.html

Dovat, N. Se creará el Centro Nacional de Operaciones de Ciberseguridad. (20 de diciembre de 2016). *La Diaria*. Recuperado de https://ladiaria.com.uy/articulo/2016/12/se-creara-el-centro-nacional-de-operaciones-de-ciberseguridad/

Hall, A. (s.f). *Tipos de delitos informáticos: los tipos de delitos informáticos reconocidos por Naciones Unidas.* Recuperado de http://www.forodeseguridad.com/artic/discipl/disc_4016.htm

Hernández, J. (2018). *Estrategias nacionales de ciberseguridad en Améica Latina*. Recuperado de http://www.seguridadinternacional.es/?q=es/content/estrategias-nacionales-de-ciberseguridad-en-am%C3%A9rica-latina

ITU (2017). *Global Cybersecurity Index (GCI) 2017*. Recuperado de https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf

Keohane, R., Nye. J., (1989). Poder e independencia. California: Foresman.

Leiva, E. (octubre, 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, volumen 3, número 4. Recuperado de revistas.unla.edu.ar/software/article/view/775

Lobato, L. (2017). La política brasileña de ciberseguridad como estrategia de liderazgo regional. URVIO - Revista Latinoamericana de Estudios de Seguridad. N.° 20, junio de 2017, pp. 16-30. Recuperado de http://revistas.flacsoandes.edu.ec/urvio/article/view/2576/2104

Machín, N., Gazapo, M., (octubre, 2016). La ciberseguridad como factor crítico en la seguridad de la Unión Europa. Revista UNISCI, número 42. Recuperado de https://www.ucm.es/data/.../UNISCIDP42-2NIEVA-MANUEL.pdf

Ministerio del Interior y Seguridad Pública (Chile) (9 de marzo de 2018). Ministerio de Defensa Nacional aprueba Política de Ciberdefensa. Diario Oficial de la República de Chile, recuperado de http://www.diariooficial.interior.gob.cl/publicaciones/2018/03/09/42003/01/1363153.pdf

Muñoz, L. Ciberseguridad, un nuevo desafío para Chile (13 de setiembre de 2018). *Estrategia.* Recuperado de http://www.estrategia.cl/texto-diario/mostrar/1183990/ciberseguridad-nuevo-desafio-chile

Observatorio de la Ciberseguridad en América Latina y el Caribe (2016). *Ciberseguridad ¿Estamos preparados en América Latina y el Caribe?* Recuperado de

https://www.agesic.gub.uy/innovaportal/file/5396/1/ciberseguridad-estamos-preparados-en-america-latina-y-el-caribe.pdf

OEA (1948). *Carta de la Organización de los Estados Americanos (A-41).* Recuperado de http://www.oas.org/es/sla/ddi/tratados_multilaterales_interamericanos_A-41_carta_OEA.asp

OEA (s.f). Comité Interamericano contra el Terrorismo (CICTE). Recuperado de http://www.oas.org/es/sms/cicte/default.asp

OEA (2014). Directorio de puntos de contacto de delito cibernético de la OEA. Recuperado de https://www.oas.org/juridico/spanish/cyber/cyber_directory.pdf

OEA (s.f). *La Red G8 24/7 Para la Conservación de Información, Declaración de Protocolo.* Recuperado de http://www.oas.org/juridico/english/cyb_pan_G8_sp.pdf

OEA (s.f). *Reportaje. Ciberdelito: 90.000 millones de razones para perseguirlo*. Recuperado de http://www.oas.org/es/centro_noticias/comunicado_prensa.asp?sCodigo=C-063/16

OEA (2004). *Resolución AG/RES. 2004 (XXXIV-O/04) "Adopción de una estrategia interamericana integral para combatir las amenazas a la seguridad cibernética: un enfoque multidimensionales y multidisciplinario para la creación de una cultura de seguridad cibernética"*. Recuperado de http://www.oas.org/en/citel/infocitel/julio-04/ult-ciberseguridad_e.asp

Ojeda Pérez, J., Rincón Rodríguez, F., Arias Flórez, M., Daza Martínez, L. (2010). *Delitos informáticos y entorno jurídico vigente en Colombia.* Recuperado de http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0123-14722010000200003

Piedras, G. (2009). CITEL: Promoviendo cooperación en ciberseguridad y protección de lainfraestructura crítica. Recuperada de https://www.itu.int/ITU-D/cyb/events/2009/santo-domingo/docs/PIERDRAS-CITEL-overview-nov-09.pdf

Piñera firma proyecto de Delitos Informáticos y anuncia instructivo de ciberseguridad para el Estado (25 de octubre de 2018). *24 horas*. Recuperado de https://www.24horas.cl/nacional/pinera-firma-proyecto-de-ley-de-delitos-informaticos-y-anuncia-instructivo-presidencial-de-ciberseguridad-para-el-estado-2845605

Portal del Estado Uruguayo (2018). Curso de Ciberdefensa y Ciberseguridad. Recuperado de https://tramites.gub.uy/ampliados?id=3847

Presidencia de la República (s.f). *CERTuy, Cometidos*. Recuperado de https://www.gub.uy/centro-nacional-respuesta-incidentes-seguridad-informatica/institucional/cometidos

Presidencia de la República (Uruguay) (2009). *Decreto N° 451/009: Centro Nacional de Respuesta a Incidentes de Seguridad Informática. Funcionamiento y Organización.* Recuperado de IMPO, Centro de Información Oficial.

Presidencia de la República (Uruguay) (2015). *Decreto N° 36/015: Creación del Centro de Respuesta a Incidentes de Seguridad Informática en el Ministerio de Defensa Nacional (D-CSIRT).* Recuperado de IMPO, Centro de Información Oficial.

Presidencia de la República (Uruguay) (2009). *Decreto N° 450/009: Principios y Líneas Estratégicas para el gobierno en red. Aprobación.* Recuperado de IMPO, Centro de Información Oficial.

Presidencia de la República (2014). *Decreto N° 92/014 del 7 de abril de 2014: Reglamentación del art. 149 de la Ley 18.719 relativo a la estandarización de los nombres de dominio de la administración central, para todos los servicios vinculados con internet.* Recuperado de https://www.agesic.gub.uy/innovaportal/v/6606/1/agesic/decreto-n%C2%B0-92_014-del-7-de-abril-de-2014.html

Presidencia de la República (Uruguay). Ejecutivo remitió al Parlamento proyecto de Ley que pena los delitos cibernéticos (30 de mayo de 2014). Recuperado de https://www.presidencia.gub.uy/comunicacion/comunicacionnoticias/seguridad-informatica-proyecto-ley

Rees, A. (2007). *Red 24/7 para Delitos de Alta Tecnología.* Recuperado de http://www.oas.org/juridico/spanish/cyb20_network_sp.pdf

REMJA (2004). Conclusiones y recomendaciones de la REMJA V, OEA/Ser.K/XXXIV.5 REMJA-V/doc.7/04 rev. 4. Recuperado de http://www.oas.org/juridico/spanish/remjaV_recomend.pdf

REMJA (2006). Conclusiones y recomendaciones. OEA/Ser.K/XXXIV.6 REMJA-VI/doc.21/06 rev. 1. Recuperado de http://www.oas.org/juridico/spanish/moj_vi_recom_sp.pdf

REMJA (2012). Documento sobre el proceso de las REMJA "Documento de Washington" OEA/Ser.K/XXXIV.7.1 REMJA-VII/doc.6/08 rev. 2. Recuperado de http://www.oas.org/juridico/spanish/doc_washington_VII_sp.pdf

Salomón, M. (junio, 2002). La Teoría de las Relaciones internacionales en los albores del siglo XXI: diálogo, disidencia, aproximaciones. Revista Electrónica de Relaciones Internacionales, número 4. Recuperada de http://www.reei.org/index.php/revista/num4

Sojo, E. (2006). Políticas públicas en democracia. México: Fondo de Cultura Económica.

UNODC (febrero, 2013). *Estudio exhaustivo sobre el delito cibernético*. Recuperado de https://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime_Study_Spanish.pdf

Uruguay y países de la OEA buscan unidad en ciberseguridad. (26 de setiembre de 2017). *El País*. Recuperado de https://www.elpais.com.uy/vida-actual/uruguay-paises-oea-buscan-unidad-ciberseguridad.html

Viega, M., Carnikian, F., (2010). *Respuestas a los delitos informáticos: su visión desde la privacidad y la seguridad de la información*. Recuperado de http://mjv.viegasociados.com/wp-content/uploads/2011/05/Cartagena-RIPD-Ciberdelincuencia-y-privacidad.pdf

Vitelli, M (2014). *Veinte años de constructivismo en relaciones internacionales. Del debate metateórico al desarrollo de investigaciones empíricas. Una perspectiva sin un marco de política exterior.* Recuperado de http://www.scielo.org.ar/scielo.php?script=sci_arttext&pid=S1851-96012014000100005

Wendt, A. (1999). Teoría social de la política internacional. Reino Unido: Universidad de Cambridge.