Uruguay y la ciberseguridad: entre los determinismos regionales y el proceso doméstico

Mónica Nieves

"El ciberespacio cuestiona toda experiencia histórica.
Es ubicuo pero no amenazante en sí mismo;
su amenaza depende de cómo se lo use"
Henry Kissinger, "El nuevo orden mundial"

Resumen

En línea con estrategias y recomendaciones sobre ciberseguridad de la Organización de Estados Americanos (OEA), Uruguay ha tomado decisiones y realizado ciertas acciones que contemplan las exigencias en la materia. En este camino, estas y otras medidas han favorecido que Uruguay se posicione a la vanguardia mundial desde el Sur Global en gobierno digital.

Este artículo aborda la construcción de la gobernanza de ciberseguridad en Uruguay. Una mirada desde las Relaciones Internacionales al desarrollo de políticas públicas domésticas y hacia el exterior en clave de ciberseguridad, implementadas por el Estado uruguayo de 2003 a 2019. Esto permitirá presentar el estado de situación y un primer acercamiento a la identificación ciertas fortalezas y debilidades identificables en la generación de respuestas de ciberseguridad como problema público.

Palabras clave: Uruguay; OEA; Ciberseguridad; Políticas públicas; Política exterior; Internet; Ciberespacio

INTRODUCCIÓN

En lo que va del Siglo XXI la seguridad como tema de agenda internacional retomó un protagonismo incuestionable. América Latina (AL) acordó en 2003 sobre la multidimensionalidad de la seguridad, en el marco de la Conferencia Especial de Seguridad de México de la OEA.

En tanto, el fenómeno Internet como determinante en la globalización, ha provocado la generación de un escenario diferente y complejo que se evidencia en el desarrollo -en palabras de Rafael Calduch- de una sociedad virtual "basada en la interconectividad comunicativa directa, instantánea,

mundial, masiva y multidimensional entre las personas" (2018: 35)[1].

Desde una perspectiva global, el desarrollo de Internet ha impulsado que las estrategias nacionales de muchos Estados entiendan a la ciberseguridad como un eje clave en la generación de políticas públicas domésticas, que tampoco debe desconocerse en el proceso de toma de decisiones de política exterior. En general ha sido el Estado el que ha potenciado el uso de Internet, ya que la inter-conectividad se ha valorado como indicador de desarrollo, y por tanto los Estados promueven mayor y mejor conectividad, cobertura territorial y accesibilidad de la población. En estos términos las ventajas del acceso y uso de Internet no suele cuestionarse. En Uruguay la penetración de Internet no solo ha ido en aumento sino que es casi del 100 % al año 2019. Más aún, 10 de cada 4 personas usan Internet en todo momento, y el 85% de los encuestados[2] usa Internet todos los días[3] (CUTI, 2019).

A su vez Internet ha determinado que sus usuarios posean lo que podría llamarse una existencia bidimensional: la *off-line* y la *on-line.* En ese sentido, el Estado se ve obligado a adaptar los marcos regulatorios existentes, o en su defecto elaborar nuevos para la sociedad virtual, con el objetivo de resguardar su soberanía, y proyectarla desde su manifestación doméstica e internacional a la virtual. Todavía hay mucho camino por recorrer en ese sentido.

La ciberseguridad es un fenómeno interméstico, que en política exterior atraviesa de manera transversal lo que Russell (1990) define como sus dimensiones político-diplomática, militar-estratégica y económica[4]. En este sentido, el ciberespacio se revela como un escenario dinámico donde el ejercicio de la soberanía se interpela constantemente en sus diversas expresiones, y en particular en lo que refiere a la seguridad. En esa línea la ciberseguridad entendida como un problema público, requerirá la generación de estrategias o políticas públicas afines.

A poco más de tres décadas desde la aparición de una noción de "ciberespacio" independizada de la ciencia ficción, los principales centros urbanos del mundo comienzan a incursionar en su fusión con el espacio físico. Aunque Kissinger (2016) avizoraba que ese fenómeno probablemente se globalizaría antes del fin de la década, es de prever que si no se ha dado aún lo hará en un futuro muy cercano.

En un mundo interconectado digitalmente al hacer foco en el Estado, éste aparece como una parte de una extraordinaria red en la que interaccionan multiplicidad de actores internacionales, con roles que difieren del tradicional en que la territorialidad es un elemento clave para el ejercicio de los atributos soberanos. Por tanto, en un contexto donde la inminencia de la transnacionalidad obliga a considerar que en el ciberespacio se conjugan de manera singular intereses públicos y privados, es imprescindible

1 Calduch sostiene que esta sociedad es distinta de las determinadas territorialmente, organizadas políticamente en Estados, para las que la lengua y la religión común son factores aglutinadores.

2 Datos surgidos de La 5ª Encuesta de Conocimientos, Actitudes y Prácticas de Ciudadanía Digital de mayo de 2019. Este estudio anual apunta a relevar el comportamiento de los uruguayos en uso y habilidades de las Tecnologías de Información y Comunicación (TIC), la confianza en la interacción digital con los servicios del Estado y con privados, etc. A partir de este análisis, se extraen datos sobre acceso y uso de Internet entre los uruguayos, realización de trámites en línea, satisfacción entre los usuarios, etc. Cabe destacar que el universo son mayores de 18 años de todo el país, y la muestra es de 1000 encuestados, con un margen de error de +-3%.

3 https://www.cuti.org.uy/novedades/1195-aumento-la-penetracion-de-internet-en-uruguay-que-es-de-casi-100-segun-encuesta. Consultada en: diciembre 2019.

4 Para Roberto Russell, la política exterior es "(…) el área particular de la acción política gubernamental que abarca tres dimensiones analíticamente separables – político-diplomática, militar-estratégica y económica – y que se proyecta al ámbito externo frente a una amplia gama de actores e instituciones gubernamentales y no gubernamentales (...)" (Russell, 1990, p. 255).

tomar en cuenta a todos los actores de la sociedad virtual a la hora ahondar en sus interacciones y entender como se dan sus relaciones de poder.

Este análisis busca identificar las estrategias y recomendaciones en ciberseguridad[5] emanadas de la OEA que han sido adoptadas en Uruguay, a la vez que explora la manera en que han sido incorporadas y desarrolladas a nivel doméstico.

Este abordaje sobre la construcción de la gobernanza de ciberseguridad en Uruguay se realiza desde de la mirada de las Relaciones Internacionales, con el fin de presentar el estado de situación que permita un primer acercamiento a un tema complejo de múltiples dimensiones.

La interrogante que se desprende es sobre la existencia de una política de ciberseguridad en Uruguay. A través del análisis cualitativo basado en la exploración documental y bibliográfica, se ha definido para el estudio el lapso que va desde el año 2003 hasta mediados de 2019.

El trabajo se estructura en cuatro partes. En primer lugar se desarrollan algunos antecedentes generales del tema de estudio, junto a líneas teóricas que se entienden aportan al entendimiento del tema elegido. A su vez se realizará un breve desarrollo del marco conceptual elemental. En segundo lugar, se aborda la ciberseguridad en función de los actores involucrados y sus implicancias. A continuación se hace analiza el determinismo multilateral regional sobre ciberseguridad a través de los desarrollos de la OEA. Seguidamente se describirá de manera general el estado de situación y en particular la experiencia de Uruguay. Finalmente se esbozan algunas reflexiones.

CONSIDERACIONES PRELIMINARES

Previo a la reunión de la Conferencia Especial de Seguridad de México de 2003, Uruguay planteó[6] que las amenazas y desafíos a la seguridad eran de origen heterogéneo. De hecho, fue un paso más allá y explicó que los instrumentos e instituciones de la OEA si bien eran necesarios frente a las llamadas amenazas tradicionales, no lo eran frente a nuevas amenazas, las que en ese momento ejemplificó en el narcotráfico (OEA, 2002).

A más de una década y media del acuerdo entre los Estados Miembros de la OEA sobre la multidimensionalidad de la seguridad, claramente es la dimensión cibernética la que demuestra una dinámica inusitada y una incuestionable conexión con el resto de las dimensiones.

La revolución tecnológica y la reestructuración del sistema capitalista como determinantes de la globalización, provocaron la aparición de una nueva dimensión en la sociedad internacional a través de la superación del tiempo y la instantaneidad en las interacciones, lo que Celestino Del Arenal denomina "tiempo global" (2008: 219). Estas ideas entran en consonancia con la de sociedad virtual -desarrollada por Rafael Calduch-, que en definitiva será el escenario principal[7] en el que se despliega el fenómeno de la ciberseguridad.

5 Para los efectos de este análisis, se utilizarán los conceptos ciberseguridad y seguridad cibernética indistintamente.

6 En el "Cuestionario sobre nuevos enfoques de seguridad hemisférica" realizado por la OEA en el año 2001. (CP/CSH-439/02)

7 Se hace referencia a un "escenario principal" en el entendido de que también hay una dimensión física que es muy importante en ciberseguridad, y en lo que por las características de este trabajo no se profundizará.

Ciertamente la coyuntura de política internacional del fin de la bipolaridad fue determinante en la inauguración de los nuevos debates a nivel global sobre una reconceptualización de la seguridad. A partir de los estudios críticos de la escuela de Copenhague y la investigación sobre el significado y alcance de la seguritización, se han ofrecido aportes muy importantes en ese sentido[8]. Para la mirada sobre las políticas públicas vinculadas ciberseguridad, el concepto de seguritización[9] presente en los trabajos de Barry Buzan, Ole Wæver, y Jaap de Wilde[10] es en una importante herramienta de análisis. Esta reposa en la idea de que los asuntos seguritizados deben estar politizados y formar parte de las políticas públicas, de manera de ser sometidos a los procedimientos regulatorios formales de la estructura gubernamental (Buzan, et al. 1998). Desde esta óptica se busca entender como un determinado hecho político deja de serlo para transformarse en un potencial riesgo de seguridad.

En clave del concepto de multidimensionalidad de la OEA, la politización de los asuntos *seguritizados* tendería a controlar una amplitud desmedida en la noción de seguridad, así como la indeterminación de amenazas o situaciones que pudieran transformarse a amenazas, ya que de lo contrario excederían al control o capacidad del Estado. A pesar del revisionismo crítico que Ole Wæver realiza al concepto de seguridad y de las diferentes agendas de seguridad, sostiene que la carga histórica y conceptual del mismo determinan su nexo con la defensa y el Estado (1998).

Proponer la ciberseguridad como un problema público implica que cierto colectivo con potencial influencia sobre actores de poder, la entiende como una situación no aceptable sobre la que es necesaria de intervención (Jaime et al., 2013). En esa línea, se asume la política pública desde la perspectiva pluralista y como resultado de un análisis del proceso de decisión.

En suma, la política pública es "(…) resultado de la confrontación entre los distintos grupos de interés implicados en los procesos de producción social" (Jaime et al.: 7). De acuerdo a Jenkins la política pública alude al conjunto de decisiones interrelacionadas que toman ciertos actores en el ámbito de su autoridad, sobre metas y medios para alcanzarlas en una situación específica (citado en: Olavarría Gambi, 2007).

A pesar de la inexistencia de consenso sobre la definición de ciberseguridad, para este trabajo se adopta aquel que refiere a la seguridad de la información digital almacenada en redes electrónicas[11]. El concepto de ciberseguridad tiene un alcance político o vinculado a la seguridad nacional (Comnimos, 2013).

Mas allá de la consideración de la ciberseguridad como política pública, la particularidad de esa dimensión de la seguridad obliga a encontrar el diálogo interdisciplinario y de perspectivas para la reflexión. Esto es así en política exterior, ya que atraviesa lo político-diplomático, militar-estratégico y económico, tiene que ver con lo público y lo privado, con el ejercicio de los derechos humanos, entre otras implicancias.

8 Avances destinados a los estudios europeos, pero que se han aplicado para los Estudios Internacionales de Seguridad (EIS).

9 Se ha optado por el concepto "seguritización" para la referencia al de "securitazation". Diversos estudios lo incluyen, aunque en su lugar también se ha utilizado la palabra "securitización"

10 En *Security. A new framework for analysis* de 1998. El concepto de seguritización es considerado una importante innovación central de los desarrollos de la Escuela de Copenhague.

11 Principalmente por entenderla como una de las definiciones más generales y adecuadas, lo que resulta muy importante a la hora de trabajar con una dimensión tan dinámica.

Siendo el Estado el tradicional garante de los derechos humanos, en un escenario en el que es imprescindible contemplar el rol de los actores no estatales en la distribución del poder estructural, tanto desde la perspectiva del poder estructural[12], como a partir de la idea de seguritización[13], se asume que la seguridad está atada al Estado. El enfoque de Susan Strange de fines de los años ochenta sobre la estructura de seguridad basada en el Estado-nación, ayuda a entender como el poder se ha desplazado a actores privados.

A su vez, la óptica de la seguritización apoya el análisis en que se presenta una concepción discursiva de la seguridad, donde las amenazas son construcciones sociales a partir del conocimiento y de los discursos que las muestran como tales. El fenómeno de la ciberseguridad podría ser incluida dentro de la noción de macro-seguritización que apunta a procesos de seguritización a escala superior y con estructuras más complejas (Verdes-Montenegro Escánez, 2013)

Asumir que la seguridad hace a la esencia del Estado desde su conformación simplificaría su abordaje, aunque la seguridad ampliada, la inminencia de la transnacionalidad, sus dinámicas y el desarrollo de la sociedad virtual lo complejizarían.

ALGUNOS DILEMAS PARA EL ESTADO

La ciberseguridad y las políticas públicas afines están condicionadas por una imprescindible vinculación/colaboración entre el sector público y privado. Esto quiere decir que en lo que refiere a la ciberseguridad, junto al Estado deberán trabajar las corporaciones vinculadas a las tecnologías de la información, la academia, pero también las ONG's y la sociedad civil nacional e internacional.

Las transformaciones determinadas por la tecnología cuestionan profundamente no solo el concepto de frontera, sino que plantean una crítica teórica esencial a la noción de lo "internacional". Hablar de ciberseguridad obliga a cuestionar y repensar el concepto de frontera, en función de los fenómenos de desterritorialización y re-territorialización "de los espacios de poder tradicionales" (Del Arenal, 2008: 220). Los Estados padecen los perjuicios latentes del llamado *malware,* lo que demuestra la invalidez de las fronteras, lo que suma complejidad al efectivo ejercicio de los atributos soberanos del Estado.

En clave de sociedad virtual, cada vez son más los autores que aceptan que el territorio ha dejado de ser un elemento categórico para la interacción social y el ejercicio de la autoridad política[14]. En este sentido la presencia física y movilidad de los actores no es imprescindible y la presencia corporal de los agentes durante la acción ya no es un requerimiento básico (Huguet Santos, 2001). Esta idea es esencial a la hora de discutir sobre el delito cibernético, que tanto complica a las legislaciones nacionales y en particular a las de los Estados miembros de OEA, en tanto solo diez de ellos han suscrito el

12 Ampliar en: *States and markets*, de Susan Strange (1998)

13 Desde la escuela de Copenhague y la investigación sobre el significado específico de la seguritización, se han realizado los aportes más importantes para la conceptualización de la seguridad, particularmente para los estudios europeos y en general para los Estudios Internacionales de Seguridad (EIS).

14 Santos Belandro, R. B. (2013). Territorio, frontera, soberanía y espacios: Cuatro conceptos que tensionan al derecho internacional privado

Convenio de Budapest[15].

En suma, la generación de políticas de ciberseguridad efectivas y eficientes se condiciona por la desterritorialización de las amenazas y por la naturaleza dispersa de los distintos riesgos que enfrentan los Estados.

En palabras de Kissinger "La tecnología de internet ha superado la estrategia y la doctrina" (2016: 344). Escenarios de gran complejidad como consecuencia de la infinidad de riesgos que sobre los activos de información críticos de los Estados[16], se darán cada vez con mayor asiduidad, y en diferentes niveles de gravedad. Esta situación obliga a los Estados a elaborar protocolos y marcos de ciberseguridad que contemplen lineamientos nacionales e internacionales, públicos y privados.

A su vez la tecnología y los servicios que son la base principal en la evolución de la sociedad virtual, no son en general controlados por los Estados. Dependen de actores internacionales transnacionales, que son capaces de redefinir las manifestaciones de la libertad y el ejercicio de la soberanía de los Estados (Sabiguero et al., 2016), y por tanto delinear nuevos parámetros en términos de ciberseguridad. Las iniciativas vinculadas a la ciberseguridad podrían ser fuente de poder tanto de corporaciones como de gobiernos, para realizar espionaje sobre los usuarios (Comninos, 2013).

Las políticas de ciberseguridad implementadas por los Estados, su consecuente capacidad y potencialidad de control sobre los derechos de los individuos, implica un muy delicado equilibrio entre la garantía de seguridad y el pleno ejercicio de las libertades.

El Determinismo Multilateral Regional: la OEA y la Seguridad Cibernética

La seguridad cibernética es un tema en el que ha incursionado tempranamente la OEA. Tal es así que se ha convertido en la primera organización internacional regional en adoptar un documento vinculado a esa temática a principios del siglo XXI. De hecho, recién en 2013 la Unión Europea (UE) logró alcanzar un acuerdo similar entre sus miembros.

En 2004 fue aprobado en el marco de la OEA el documento para la "Adopción de una Estrategia Interamericana Integral de Seguridad Cibernética: Un Enfoque Multidimensional y Multidisciplinario para la Creación de una Cultura de Seguridad Cibernética". Será la Secretaría del Comité Interamericano contra el Terrorismo (CICTE), la mandatada[17] para trabajar sobre asuntos de Seguridad Cibernética. En particular esta Secretaría estará a cargo de la construcción de capacidades de ciberseguridad en los Estados miembros, a través de un enfoque integral en el que confluirán responsabilidades nacionales e internacionales, entidades públicas y privadas de los Estados, abocadas a los aspectos técnicos y

15 Convenio sobre Ciberdelincuencia de la Unión Europea, que propone la homogenización la conceptualización de la ciber-criminalidad y todo lo vinculado a ese fenómeno. Tratado vinculante en materia penal, que entiende sobre la necesidad de aplicar una política penal común.

16 Activos de información necesarios para asegurar y mantener el correcto funcionamiento de los servicios vitales para la operación del gobierno y la economía del país.

17 Por la resulución AG/RES. 2004 (XXXIV-O/04). Disponible en: http://www.oas.org/juridico/spanish/ag04/agres_2040.htm. Consultada: mayo, 2017

políticos para “asegurar el ciberespacio”[18].

En pos de considerar las particularidades de cada Estado miembro -en tanto asimetrías y por ende diferentes necesidades, sensibilidades y vulnerabilidades-, ante las solicitudes de asistencia técnica, la Secretaría del CICTE ha instrumentado un sistema de evaluaciones que identifican los requerimientos nacionales. El objetivo es encontrar las herramientas necesarias para el fortalecimiento de la ciberseguridad (Ibarra, Nieves, 2016)

A su vez esta Secretaría no solo está a cargo del establecimiento de los Equipos de Respuesta a Incidentes (CSIRT) en cada Estado miembro, sino que le compete la creación de una red de alerta hemisférica, así como el desarrollo de Estrategias Nacionales sobre Seguridad Cibernética. Es de destacar la referencia que se hace al fomento del desarrollo de una “cultura” para el fortalecimiento de la ciberseguridad hemisférica[19]. El énfasis en la responsabilidad de las autoridades para la promoción de la creación de una “cultura de la seguridad cibernética”, ha sido un tema presente desde hace varios años[20](OEA, SYMANTEC, 2014).

El programa de Ciberseguridad de OEA-CICTE se ha centrado en tres ejes que refieren al desarrollo de políticas, al desarrollo de capacidades, a la investigación y divulgación. A través de este programa se ha participado en múltiples foros internacionales, en función del reconocimiento de la importancia de cooperación internacional y de la participación en iniciativas internacionales vinculadas a la ciberseguridad. En este sentido, desde el año 2004 se ha apoyado la creación y participación de los CSIRT, este trabajo se apuntaló a partir del 2016 con el lanzamiento una plataforma virtual para los CSIRT (s.f.: OEA)[21]

Es a partir de la identificación de un “ecosistema informático de América Latina y el Caribe” (OEA, SYMANTEC, 2014), que la OEA ha enfatizado en favorecer la cooperación entre el sector público, privado, académico y los usuarios finales. En este sentido, los Estados deben promover una cultura de ciberseguridad y actuar en pos de la protección de los usuarios individuales, que en definitiva son los actores más vulnerables.

El documento de la Estrategia Interamericana Integral de Seguridad Cibernética también da marco en su actuación a la Comisión Interamericana de Telecomunicaciones (CITEL), así como al Grupo de Expertos Gubernamentales en materia de Delito Cibernético de la Reunión de Ministros de Justicia de Ministros Procuradores Generales de las Américas (REMJA)[22], junto a otros órganos. La coordinación de la Estrategia queda a cargo del Consejo Permanente a través de la Comisión de Seguridad Hemisférica[23] (CITEL, 2014).

El CICTE se ocupará de la creación de una red hemisférica que funcione las 24 horas, los siete días de la semana. Las principales características de la iniciativa para dicha red, así como el plan de acción, se

18 Ampliar en: https://www.sites.oas.org/cyber/Es/Paginas/default.aspx

19 Ibid

20 Como lo ha sostenido reiteradamente el ex Secretario de Seguridad Multidimensional de la OEA Adam Blacwell

21 http://www.oas.org/es/sms/cicte/prog-ciberseguridad.asp#myActividades. Consultada: mayo, 2019

22 AG/RES. 2004 (XXXIV-O/04). Disponible en: http://www.oas.org/juridico/spanish/ag04/agres_2040.htm. Consultada: mayo, 2017

23 Ibid

describen en el documento “Recomendaciones del Taller de Practicantes en Materia de Seguridad Cibernética del CICTE sobre la Estrategia Integral de Seguridad Cibernética de la OEA: Marco para establecer una Red Interamericana CSIRT de Vigilancia y Alerta” (CICTE, 2004)[24].

La Resolución denominada “Seguridad cibernética”, guía la labor de la CITEL y entiende que su contribución a la Estrategia Interamericana Integral sobre Seguridad Cibernética “adoptará un enfoque prospectivo y buscará fomentar el intercambio de información entre los Estados Miembros para así promover las redes seguras”[25]. En tanto, esta Comisión realizará recomendaciones para la adopción de normas de seguridad de especial importancia a los Estados miembros. CITEL tendrá un importante rol en la difusión de información técnica y práctica en ciberseguridad (CITEL, 2014).

Por su parte la REMJA auxilia a la Estrategia, en tanto busca asegurar que los Estados miembros de la OEA cuenten con instrumentos jurídicos que protejan a los usuarios de Internet y las redes de información. Para alcanzar ese objetivo, asistirá a los Estados miembros en el combate al delito cibernético, a través del Grupo de Expertos que facilitará a las autoridades policiales y judiciales herramientas jurídicas necesarias, asistencia técnica en la redacción de leyes que tipifiquen el delito informático, y la promoción de mecanismos jurídicos que fomenten la cooperación en temas vinculados a los delitos cibernéticos (CITEL, 2014).

ESTADO DE SITUACIÓN Y LA EXPERIENCIA DE URUGUAY

En el informe Ciberseguridad 2016 ¿Estamos preparados en América Latina y el Caribe?[26], se expresa que la región presenta vulnerabilidades "potencialmente devastadoras" (BID-OEA, 2016). Esto es así ya que según el análisis de los indicadores regionales realizado por el Observatorio, cuatro de cada cinco Estados “no tienen estrategias de ciberseguridad o planes de protección de infraestructura crítica”(p.IX).

El informe estima que deben reforzarse los aspectos vinculados a la política y estrategia de ciberseguridad de toda América Latina y el Caribe (ALC), especialmente en lo que refiere a la protección de las infraestructuras críticas. Asimismo, enfatiza en la creación de canales de cooperación a distintos niveles entre los gobiernos nacionales, las organizaciones internacionales mundiales y regionales vinculadas a la temática. Reconoce la importancia de la cooperación internacional y la armonización legal en el ámbito de Internet, donde no existen las fronteras.

Uno de los análisis de expertos del informe es el de James A. Lewis[27], que es categórico al afirmar que “Hacer frente a estos desafíos requiere de esfuerzos diplomáticos y la cooperación internacional. Algo que hemos aprendido en seguridad cibernética es que ninguna nación por sí sola puede asegurar adecuadamente sus redes. La cooperación es esencial” (BID-OEA, 2016: 4). Asimismo, Lewis reseña los foros de discusión internacional sobre las normas en ciberseguridad, las medidas de generación de

24 CICTE/REGVAC/doc.2/04

25 CCP.I/RES.49 (IV-04)

26 Análisis llevado a cabo en colaboración entre el Banco Interamericano de Desarrollo (BID), la Organización de los Estados Americanos (OEA) y el Centro Global de Capacitación de Seguridad Cibernética (GCSCC) de la Universidad de Oxford.

27 Director y Miembro Senior, Programa Estratégico de Tecnologías, del Centro de Estudios Estratégicos e Internacionales (CSIS)

confianza y la creación de capacidades, seleccionando cuatro grupos multilaterales: el Grupo de Expertos Gubernamentales de Naciones Unidas (GEG), la Organización para la Seguridad y la Cooperación en Europa (OSCE), el Foro Regional de la Asociación de Naciones del Sureste Asiático (ASEAN) y la OEA.

De esta manera se evidencia el compromiso multilateral y de cooperación que la OEA esgrime en materia de ciberseguridad. Sin embargo no debe obviarse que el informe insiste en la importancia contemplar a los grupos de la sociedad civil, la academia, los técnicos, el sector privado, industrial, ya que desde su experiencia y perspectiva pueden aportar al diseño de un "marco reglamentario racional de una manera sostenible" (BID-OEA, 2016: 10).

Asimismo el informe enfatiza que en términos generales, una estrategia nacional de ciberseguridad requiere que los Estados cuenten con un órgano de coordinación de Presidencia para "supervisar la aplicación, coordinar las gestiones de las entidades" (BID-OEA, 2016: 6). A su vez la estrategia determinará la responsabilidad para la seguridad cibernética de los distintos ministerios. Estos serán los que se vincularán y colaborarán con el sector privado, indicando específicamente a los sectores relacionados con la energía eléctrica, las telecomunicaciones y las finanzas.

Por otra parte el informe entiende que los gobiernos nacionales requieren de "(…) organizaciones de seguridad cibernética adecuadamente atendida que incluyan como mínimo un CERT nacional y policía cibernéticamente capaz". El compromiso en cooperar y trabajar integralmente se remarca en el documento, afirmando "(…) que todas las naciones se benefician del intercambio de mejores prácticas y de información sobre amenazas y vulnerabilidades" (OEA, BID, 2016: 6)

Un reciente trabajo de la OEA –el quinto de la serie *White paper-,* rescata los avances realizados en Estados Unidos (EE.UU) vinculados al desarrollo de su *Cybersecurity Framework* (CSF), y presenta las utilidades del CSF para otros Estados. A principios de 2013, por medio de la orden ejecutiva 13636, el presidente Barack Obama requirió que el Instituto Nacional de Estándares y Tecnologías (NIST) elaborara el CSF[28].

La OEA sostiene que el CSF contribuye en la "(…) elaboración de estrategias de ciberseguridad de los gobiernos (en particular, en la protección de sus infraestructuras críticas) y en fortalecer los procesos de colaboración regional" (OEA, 2019: 8). A pesar del impulso de la OEA al CSF, y que este ha sido adoptado por varios Estados en el mundo, solo lo han hecho dos de sus Estados miembros: EE.UU y Uruguay.

I. El caso de Uruguay

La Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento (AGESIC)[29] es una unidad ejecutora dependiente de Presidencia de la República Oriental del Uruguay, aunque con autonomía técnica. Fue creada por el art. 72 de la Ley No.17.930 de 2005[30]. Esta agencia tendrá un Consejo

28 En el que se identifican 16 sectores de infraestructuras críticas: químico; instalaciones comerciales; comunicaciones; fabricación crítica; presas/represas; base industrial de defensa; servicios de emergencia; energía; servicios financieros; comida y agricultura; instalaciones gubernamentales; salud y salud pública; tecnología de información; reactores nucleares, materiales y residuos; sistemas de transporte; sistemas de agua y aguas residuales.

29 Denominada originalmente: Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento

30 https://www.impo.com.uy/bases/leyes/17930-2005. Consultada: mayo, 2019

Directivo Honorario integrado por cinco miembros, y tres Consejos Asesores Honorarios. Estos Consejos estarán integrados por los rectores de las Universidades[31], autoridades de la Administración Central, varios ministros, representantes de empresas nacionales e internacionales[32] vinculadas a las tecnologías de la información y jerarcas del sector informático de los organismos estatales (Ley No.17.930 de 2005).

Reglamentada en junio de 2006 por el Decreto 205[33], AGESIC asume el objetivo de:

> "(…) procurar la mejora de los servicios al ciudadano, utilizando las posibilidades que brindan las tecnologías de la información y las comunicaciones (TIC). Asimismo, impulsará el desarrollo de la Sociedad de la Información en el Uruguay con énfasis en la inclusión de la práctica digital de sus habitantes y el fortalecimiento de las habilidades de la sociedad en la utilización de las tecnologías"

La Ley de Rendición de Cuentas 18046 de 2006 [34] (Art. 55), amplió sus objetivos y agregó las tareas de planificación y coordinación de proyectos vinculados al Gobierno Electrónico en pos de mayor transparencia del Estado, así como el desarrollo de política nacional en temas de seguridad de la información a fin de prevenir, detectar y responder a incidentes que afecten a los activos críticos nacionales.

Bajo la órbita de AGESIC fue creado el Centro Nacional de Respuesta a Incidentes de Seguridad Informática (CERTuy) -Ley 18.362 de 2008[35]-, que asiste a la Unidad de Delitos Cibernéticos de la Policía Nacional, responsable de la investigación de delitos cibernéticos y similares[36].

Los objetivos de AGESIC se han ido cumpliendo a través de tres etapas. La primera fue la etapa de institucionalización e implantación que se extendió desde 2006 a 2010. Desde 2011 a 2015, en la etapa de expansión se persiguió la universalización de las iniciativas y tecnologizar sectores estratégicos. A partir de 2016 se inició la tercera etapa llamada de transformación, que finalizará en 2020. Esta se propone el "Uso de la tecnología como motor de modelos de gestión al servicio del desarrollo sostenible y como impulsor de igualdad de oportunidades" (Presidencia de la República, s.f. a). Claramente estos objetivos han apuntado a fortalecer el desarrollo del gobierno digital, promoviendo la digitalización de la administración pública y haciendo foco en el usuario.

En el art. 8 del Decreto no. 451/009[37] se detallan los cometidos y potestades del CERTuy, así como una serie de obligaciones para este y AGESIC, entre las que se encuentran adoptar medidas de seguridad para proteger los activos críticos de información. Específicamente puntualiza en las consecuencias de los incidentes de seguridad informática, que afecten los activos de información críticos del Estado. Por

31 De la Universidad de la República (UdelaR) y de las universidades privadas.

32 Instaladas en el país.

33 https://www.impo.com.uy/bases/decretos/205-2006. Consultada, abril, 2019

34 https://www.impo.com.uy/bases/leyes/18046-2006. Consultada, mayo 2019

35 https://www.impo.com.uy/bases/leyes/18362-2008. Consultada: abril 2019

36 Ampliar en: https://www.sites.oas.org/cyber/Documents/2014%20-%20Tendencias%20de%20Seguridad%20Cibern%C3%A9tica%20en%20Am%C3%A9rica%20Latina%20y%20el%20Caribe.pdf

37 https://www.impo.com.uy/bases/decretos/451-2009/8. Consultada: abril, 2019

su parte en el art. 2 se definen: activos de información[38], activos de información críticos del Estado[39], evento de seguridad informática[40], incidente de Seguridad Informática[41], servicios vitales para la operación del gobierno y la economía del país[42].

Con el Decreto no. 452/009[43] se procura la adopción de una Política de Seguridad de la Información para Organismos de la Administración Pública, con el propósito de dar impulso a un Sistema de Gestión de Seguridad de la Información. En 2014 el Decreto no. 92 con el objetivo de mejorar la seguridad de la información y las infraestructuras tecnológicas que le dan soporte, dispone la estandarización de los nombres de dominio para los servicios vinculados con Internet de la Administración Central. La fiscalización estará a cargo de AGESIC[44].

El Decreto no. 36/015[45] crea el Centro de Respuesta a Incidentes de Seguridad Informática en el Ministerio de Defensa (D-CSIRT) que funcionará como centro coordinador de las actividades vinculadas a la gestión de incidentes de seguridad informática, en colaboración con organismos e instituciones nacionales e internacionales vinculadas a la seguridad informática, y en coordinación con CERTuy. Ha sido la OEA que mediante la Iniciativa de Seguridad cibernética, ha dado impulso para la creación del D-CSIRT, que actúa en red con organismos internacionales como CICTE.

En 2015 el Decreto no. 184[46] determinó las competencias de AGESIC, y le atribuyó ciertos poderes jurídicos vinculados a la intervención preceptiva en la elaboración de planes anuales de informática que sean confeccionados por los entes de la Administración Central.

El "Informe Ciberseguridad 2016" reveló que Uruguay se encontraba en un nivel intermedio de madurez en cuanto a preparación del Estado ante la amenaza del cibercrimen, aunque aún lejos de países avanzados como Estados Unidos o Israel. La valoración de la "madurez" de las políticas de seguridad cibernética se realizó en base a 49 indicadores de cinco áreas, a saber: política y estrategia, cultura y sociedad, educación, marco legal y tecnología (BID-OEA, 2016).

Es de destacar que a partir de febrero de 2018 Uruguay se convirtió en el primer Estado suramericano parte del *Digital 9* (D9), que también integran Canadá, Estonia, Israel, Portugal, México, Nueva Zelanda,

38 Datos o información que tienen valor para una organización.

39 Activos de información necesarios para asegurar y mantener el correcto funcionamiento de los servicios vitales para la operación del gobierno y la economía del país.

40 Una ocurrencia identificada de un estado de un sistema, servicio o red que indica una posible violación de la política de seguridad de la información, la falla de medidas de seguridad o una situación previamente desconocida, que pueda ser relevante para la seguridad.

41 Violación o una amenaza inminente de violación a una política de seguridad de la información implícita o explícita, así como un hecho que comprometa la seguridad de un sistema (confidencialidad, integridad o disponibilidad).

42 Servicios referidos a la salud, orden público, servicios de emergencia, energía, telecomunicaciones, transporte, suministro de agua potable, ecología y ambiente, agroindustria, servicios públicos, banca y servicios financieros o cualquier otro servicio que afecte a más del 30% de la población.

43 https://www.impo.com.uy/bases/decretos/452-2009. Consultada, abril, 2019

44 https://www.impo.com.uy/bases/decretos-originales/92-2014#ANEXOI. Consultada: mayo 2019

45 https://www.impo.com.uy/bases/decretos/36-2015. Consultada: abril, 2019

46 https://www.impo.com.uy/bases/decretos/184-2015. Consultada: mayo, 2019

Reino Unido y República de Corea[47]. Este foro está conformado por los gobiernos más digitalizados del mundo. En la cumbre de Jerusalén en noviembre de 2018, Uruguay asumió la presidencia del grupo (Presidencia de la República, 2019). El D9 promueve la conectividad, la ciudadanía digital, la programación desde la niñez, el gobierno abierto, los estándares y códigos abiertos y el gobierno centrado en las personas. La membresía en este foro es relevante para Uruguay, ya que lo ubica al mismo nivel de otros actores destacados y de primer orden en gobierno digital a nivel global, además que participa en una plataforma en la que se discuten asuntos trascendentes en la materia, como el desarrollo del gobierno digital, la ética de la inteligencia artificial, entre otros (Presidencia de la República, 2019).

II. La política digital y el Marco de Ciberseguridad de Uruguay

A partir de la premisa de que la seguridad es asunto interméstico por excelencia, su dimensión cibernética se muestra como vector que atraviesa las dimensiones político-diplomática, militar-estratégica y económica. En estos términos, puede verse que el gobierno uruguayo a través de AGESIC ha desarrollado una perspectiva transversal.

En enero de 2016 se lanzó la versión 1.0 del Marco de Ciberseguridad de Uruguay (MCU) basado en el CSF definido por el NIST. La versión 4.0 de enero de 2018 se alinea con las referencias a estándares internacionales y contemplan la normativa nacional. En esta última versión se contemplan especialmente las instituciones de salud -públicas o privadas-, que podrán utilizar el CSF a modo de "herramienta de autoconocimiento y mejora de sus niveles de seguridad". El MCU apunta a reducir el riesgo frente a amenazas cibernéticas que puedan comprometer la seguridad de la información[48] (Presidencia de la República, 2018).

El objetivo principal del MCU es generar confianza en el uso de la tecnología, unificar recursos en ciberseguridad existentes y soportar la evolución del gobierno digital uruguayo, en función de la promoción de una visión integral y multisectorial de ciberseguridad (OEA, 2018). El MCU apunta a apoyar a organizaciones públicas o privadas a planificar su estrategia de gestión de riesgos de ciberseguridad, de modo de poder desarrollarla de acuerdo a sus particularidades -tamaño, tipo de actividad, etc.-. Esto es posible porque este marco no es un documento estático sino que es adaptable a la evolución tecnológica, según las amenazas e incluso a contemplando la transformación de las técnicas en gestión de riesgos (OEA, 2018).

El MCU ha sido utilizado en diagnóstico y evaluación de todos los Ministerios, Gobiernos Departamentales, Instituciones de Salud y Financieras. Este documento propone a su vez -en base a los controles ISO/IEC 27001 y la normativa nacional en materia de ciberseguridad-, un conjunto de 65 requisitos. Puede ser utilizado por cualquier institución pública o privada, y aunque en la actualidad no tiene carácter obligatorio, se prevé en el corto plazo su obligatoriedad para sectores críticos (OEA, 2018).

Uruguay es considerado el país de ALC con mayor índice en relación al gobierno digital, según el reporte *E-government Survey* publicado en 2018 por Naciones Unidas. Este reporte analiza indicadores sobre el avance digital de las administraciones públicas, y coloca a Uruguay en el puesto 26° a nivel

47 Cabe destacar que este foro pasó a ser D10 o *Digital Nations* en noviembre de 2019, con la incorporación de Dinamarca. Al ser un acontecimiento fuera de la periodización determinada para el trabajo, si bien se entendió conveniente mencionarlo, será desarrollado en una próxima actualización de esta investigación.

48 En base a prácticas internacionales como: ISO/IEC 27001:2013 3 , COBIT 5 4, NIST SP 800-53 rev.4.

global según el índice de participación electrónica, y en el puesto 35° a nivel global entre los más avanzados en *E-government*. Destaca la Agenda Uruguay Digital (AUD) 2020 como ejemplo de prioridad del gobierno en la democratización del acceso a los trámites, su trazabilidad y acceso de usuario único con el Estado. Asimismo resalta el proyecto de Ventanilla Única de Comercio Exterior (VUCE) como mecanismo de facilitación del comercio exterior en términos de "rediseño del proceso de comercio exterior", soportado en la revisión normativa y la incorporación de tecnología necesaria que hace de VUCE una plataforma única de gestión (United Nations, 2018)[49].

III. LA AGENDA URUGUAY DIGITAL 2020

La llamada "política digital" de AGESIC, surge de la AUD 2020[50] en cuatro versiones, la última comprende el periodo 2016-2020. En este documento "(…) se establecen, priorizan, articulan y difunden de desarrollo de la Sociedad de la Información y el Conocimiento en la Administración Pública (...)" (Presidencia de la República, s.f. b), con el objetivo de alcanzar la transformación digital del país de manera integral. Con las medidas detalladas en la AUD 2020 se pretende construir una visión integral, coincidente con los objetivos estratégicos de desarrollo de Uruguay y a su vez que aporten a los objetivos de la Agenda de Desarrollo Sostenible 2030. Se busca la incorporación plena de la tecnología en los sectores productivos, además de la profundización del vínculo entre ciudadanía y Estado a través de un marco que promueva su desarrollo (Presidencia de la República, mayo 2019: 8)

En el plano doméstico, la Agenda toma en consideración las prioridades de política pública definidas en la planificación estratégica y presupuestal del quinquenio, mientras que en el plano internacional contempla como referentes a la Cumbre Mundial de la Sociedad de la Información (CMSI) y la Agenda Digital para América Latina y el Caribe. La AUD 2020 plantea cuatro pilares con objetivos, compromisos y metas de cumplimiento específicos. Ellos son: Políticas sociales e inclusión; Desarrollo económico sustentable; Gestión de gobierno; y Gobernanza para la sociedad de la información (Presidencia de la República, mayo 2019: 8,9).

En función de esta última Agenda, AGESIC desarrolló el Plan de Gobierno Digital 2020 que propone las líneas necesarias para implementar de manera integral la transformación digital del gobierno uruguayo. Las líneas de acción del documento de AGESIC que incluyen diecinueve objetivos, incluyen: Gobierno Cercano, Gobierno Abierto, Gobierno Inteligente, Gobierno Eficiente, Gobierno Integrado y Gobierno Digital Confiable.

En el marco del Gobierno Digital Confiable, según se expone en el objetivo XVI "Fortalecer el ecosistema de ciberseguridad" se propone la creación de un Centro Nacional de Operación de Ciberseguridad (SOC) de participación público-privada. El SOC se propone la detección en tiempo real de eventos e incidentes de ciberseguridad en los activos de información críticos del Estado, a la vez que pretende abocarse a prevenir incidentes de ciberseguridad. Además asesorará -entre otras responsabilidades- en la definición de políticas, metodologías y buenas prácticas de ciberseguridad, por lo tanto deberá

49 https://publicadministration.un.org/egovkb/en-us/Resources/E-Government-Survey-in-Media/ID/1901/Uruguay-es-l237der-en-Am233rica-Latina-y-el-Caribe-con-el-gobierno-digital-m225s-avanzado. Consultada: julio, 2019

50 https://uruguaydigital.uy/wps/wcm/connect/urudigital/6bd54ea6-1207-4cfa-bafb-c859bdac8019/Descargar+Agenda+Uruguay+Digital+2020.pdf?MOD=AJPERES&CONVERT_TO=url&CACHEID=6bd54ea6-1207-4cfa-bafb-c859bdac8019. Consultada, julio 2019

interactuar con CERTuy y otros CSIRTs –de manera de intercambiar información y coordinar operaciones de ciberseguridad-, así como con otros SOC en el intercambio y procesamiento de información y alertas de ciberseguridad (Presidencia de la República, s.f.c).

En tanto, desde mayo de 2016 el Proyecto de Ley Ciberdelincuencia y Delitos Informáticos se encuentra en estudio de la Comisión Especial de Innovación, Ciencia y Tecnología de la Cámara de Representantes, luego que en la anterior legislatura no fuera aprobado. Este proyecto que fue retomado para estudio en 2018, será tratado junto al que AGESIC presentó en 2015, y que posee similar articulado (La Diaria, mayo 2018). Entre la exposición de motivos relatada en el mismo proyecto, se hace referencia al objetivo del Convenio sobre Ciberdelincuencia de 2001 de Budapest[51] suscrito entre los miembros del Consejo de Europa y otros Estados extra-europeos, y lo incluye como antecedente (Council of Europe, s.f.)

Teniendo en cuenta lo que se ha tratado en estas páginas, en cuanto lo que implica el desarrollo de las tecnologías y estas en relación a la vida *off line / on line*, contar con una legislación específica sobre ciberdelincuencia y delitos informáticos parece ser de imperiosa necesidad. En la línea de pensamiento de Perrit (2004) se entiende que Internet no solo ha modificado la funcionalidad de las fronteras nacionales, sino también la esencia de los derechos fundamentales de raíz constitucional.

ALGUNAS REFLEXIONES FINALES

La ciberseguridad es una dimensión de la seguridad que involucra lo público y lo privado, y es transversal al resto de las dimensiones de seguridad. Atada en esencia al Estado y a la defensa, se desarrolla principalmente en un escenario en el que los roles de los actores internacionales se manifiestan de manera diferente a los tradicionales en la sociedad internacional. Todo esto interpela el ejercicio de los atributos soberanos del Estado.

Respondiendo a la pregunta planteada al inicio de este análisis sobre la existencia de una política de ciberseguridad en Uruguay, la respuesta se puede proponer desde diferentes lugares. Por un lado, Uruguay claramente se ha comprometido en adoptar las medidas y estrategias de ciberseguridad provenientes de la OEA, por lo tanto el camino de la construcción de una política pública pertinente se ha comenzado a recorrer. Resulta evidente que Uruguay se ha comprometido con la ciberseguridad, que a su vez lo destaca no solo en relación al resto de los Estados de ALC, sino a nivel global donde se coloca a la par de los Estados referentes a nivel mundial en el tema.

En la medida en que Uruguay ha seguido los lineamientos marcados por la OEA, se ha posicionado como ejemplo para otros Estados, sobre todo entre los miembros de dicha organización regional.

Algunas iniciativas parecen tener menos impulso que otras, por ejemplo la que tiene que ver con el ordenamiento jurídico, ya que aún está en el tintero desde hace varios años la Ley de Ciberdelincuencia y Delitos Informáticos, lo que además es especialmente impulsado por OEA. Asuntos tan dinámicos como el de la ciberseguridad, requiere respuestas ágiles y oportunas. Equiparar delitos informáticos a otros delitos contemplados por la legislación nacional no debiera ser una práctica que se prolongue en el tiempo, ya que la práctica internacional tiende a generar legislación específica ya que su ausencia

51 A la fecha de las sesenta y cuatro ratificaciones, diez pertenecen a Estados Miembros de la OEA: Argentina, Canadá, Chile, Costa Rica, Estados Unidos, República Dominicana, México, Panamá, Paraguay y Perú

implica un vacío legal muy cuestionable.

Parte de la explicación radica en que a pesar de que el MCU no tiene carácter obligatorio, su obligatoriedad proyectada para el corto plazo para sectores críticos, apuntalaría la construcción de una política pública.

La dinámica y complejidad de la ciberseguridad como problema público, obliga a pensar en clave de política pública de ciberseguridad construida a diferentes niveles de gobierno, e implica la participación de múltiples actores. Asimismo, se requiere de un estudio más profundo e integral a fin de evaluar tanto las acciones como las decisiones en la materia tomadas por el gobierno uruguayo a través de AGESIC, para entender el proceso y estadío del desarrollo de la política pública en ciberseguridad. Se torna imprescindible profundizar en los procesos decisiorios pertinentes en toda la estructura gubernamental. Contemplar únicamente la acción de AGESIC -y a pesar de la construcción del MCU-, no parece ser suficiente para asegurar la existencia de una política pública de ciberseguridad

En ese sentido, aparece el cuestionamiento sobre cuál es el escenario a mediano y corto plazo para Uruguay, que avanza significativamente en gobierno digital aunque no ha logrado dinamismo a nivel de legislación sobre cibercriminalidad.

REFERENCIAS BIBLIOGRÁFICAS

BID-OEA (2016). *Ciberseguridad ¿Estamos preparados en América Latina y el Caribe?* Informe Ciberseguridad 2016. Observatorio de la Ciberseguridad en América Latina y el Caribe. Disponible en: http://observatoriociberseguridad.com/graph/countries//selected//0/dimensions/1-2-3-4-5. Consultada en: abril, 2017

Buzan, B., Wæver, O., y de Wilde, J. (1998) *Security: A new framework for Analysis.* Londres: Lynne

Calduch, R. (2018) "La transición entre sociedades internacionales y el Derecho Internacional Público", en: *Anuario Español de Derecho Internacional*, no 34 (2018); Universidad de Navarra. pp. 29-50

CICTE (2004) "Estrategia de Seguridad Cibernética. Resolución". Disponible en: https://www.sites.oas.org/cyber/Documents/Estrategia-seguridad-cibernetica-resolucion.pdf. Consultada: mayo, 2017.

CITEL (2014) *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*". Disponible en: http://www.oas.org/en/citel/infocitel/julio-04/ult-ciberseguridad_e.asp. Consultada en: diciembre, 2019

Comnimos, A. (2013). Una agenda de ciberseguridad para la sociedad civil: ¿qué hay en juego?. *Temas Emergentes*. APC. Disponible en: https://www.apc.org/es/system/files/APCIssue_Cybersecurity_ES.pdf. Consultada: abril, 2017.

Conuncil of Europe (s.f.) "Chart of signatures and ratifications of Treaty 185". Disponible en: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=TAnc9gl1). Consultada: mayo 2019

CUTI (2019) Aumentó la penetración de Internet en Uruguay, que es de casi 100%, según encuesta. Disponible en: https://www.cuti.org.uy/novedades/1195-aumento-la-penetracion-de-

internet-en-uruguay-que-es-de-casi-100-segun-encuesta. Consultada en: diciembre 2019

Decreto no. 205/006. Disponible en: https://www.impo.com.uy/bases/decretos/205-2006. Consultada, abril, 2019

Decreto no. 451/009. Disponible en: https://www.impo.com.uy/bases/decretos/451-2009/8. Consultada: abril, 2019

Decreto no. 452/009. Disponible en: https://www.impo.com.uy/bases/decretos/452-2009. Consultada: abril 2019

Decreto no. 92/014. Disponible en: https://www.impo.com.uy/bases/decretos-originales/92-2014#ANEXOI. Consultada en: mayo 2017

Decreto no. 36/015. Disponible en: https://www.impo.com.uy/bases/decretos/36-2015. Consultada, abril 2019

Decreto no. 184/015. Disponible en: https://www.impo.com.uy/bases/decretos/184-2015. Consultada: mayo, 2019

Del Arenal, C. (2008) Mundialización, creciente interdependencia y globalización en las relaciones internacionales, en: *Gasteiz, V. Cursos de Derecho Internacional y relaciones Internacionales*. ISSN 1577-533X, Nº. 1, 2008, ISBN 978-84-9860-242-5, pp. 181-268

Huguet Santos, M. (2001). Historia del tiempo presente e historia de las relaciones internacionales, en J. C. Castañares (ed.). *La Historia de las Relaciones Internacionales.* pp. 48-53. Disponible en: de http://www.jstor.org/stable/41325055. Consultada en: abril, 2017

Ibarra, V., Nieves, M. (2016). "La seguridad internacional determinada por un mundo on-line: el Estado ante el desafío del terrorismo y la ciberseguridad". VIII Congreso de Relaciones Internacionales. Argentina: Instituto de Relaciones Internacionales (IRI). UNLP. Disponible en: http://congresos.unlp.edu.ar/index.php/CRRII/CRRII-VIII/paper/viewFile/3464/874. Consultada en: abril, 2017

Jaime, F.M. et al. (2013) *Introducción al análisis de políticas públicas.* 1A ed. Florencio Varela : Universidad Nacional Arturo Jauretche. ISBN 978-987-29188-3-5

Kissinger, H. (2016) *El Orden Mundial. Reflexiones sobre el carácter de los países y el curso de la historia.* Buenos Aires: Debate

La Diaria (mayo 2018) Montevideo, Uruguay "Comienzan a tratar proyectos contra ciberdelitos". Disponible en: https://ladiaria.com.uy/articulo/2018/5/comienzan-a-tratar-proyectos-contra-ciberdelitos/. Consultada: abril, 2019

Ley No.17.930 de 2005. Disponible en: https://www.impo.com.uy/bases/leyes/17930-2005. Consultada: mayo 2019

Ley N° 18046 de 2006. Disponible en: https://www.impo.com.uy/bases/leyes/18046-2006. Consultada, mayo 2019

Ley N.º 18362 de 2008. Disponible en: https://www.impo.com.uy/bases/leyes/18362-2008. Consultada: abril 2019

Russell, R. (1990) *Política Exterior y toma de decisiones en América Latina- Aspectos comparativos y consideraciones teóricas.* Buenos Aires: Grupo Editor Latinoamericano

OEA (2019) "Ciberseguridad. Marco Nist", en: White Papers Series, ed. 5. Disponible en:

https://www.academia.edu/40987298/MARCO_NIST_CIBERSEGURIDAD_Un_abordaje_integral_de_la_Ciberseguridad. Consultada: agosto, 2019

OEA (s.f.) Programa de Ciberseguridad. Disponible en: http://www.oas.org/es/sms/cicte/prog-ciberseguridad.asp#myActividades. Consultada en: mayo, 2019

OEA, SYMANTEC (2014) *Tendencias de Seguridad Cibernética en América Latina y el Caribe.* Disponible en: https://www.sites.oas.org/cyber/Documents/2014%20-%20Tendencias%20de%20Seguridad%20Cibern%C3%A9tica%20en%20Am%C3%A9rica%20Latina%20y%20el%20Caribe.pdf. Consultada en: abril, 2019

OEA (2002). Cuestionario sobre nuevos enfoques de la seguridad hemisférica: Observaciones generales. Disponible en: https://www.oas.org/csh/spanish/documentos/cp09378s04.doc (CP/CSH-439/02). Consultada en: abril 2017

Perrit, H. H. (2004). *Internet, ¿una amenaza para la soberanía?. Reflexiones sobre el papel de Internet en el fortalecimiento del gobierno a escala nacional y global*. Buenos Aires: Heliasta.

Presidencia de la República (s.f.a) Agencia de Gobierno Electrónico y Sociedad de la Información y el Conocimiento. AGESIC. Disponible en: https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/institucional/creacion-y-evolucion-historica. Consultada: abril, 2019

Presidencia de la República (s.f.b) Agencia de Gobierno Electrónico y Sociedad de la Información y el Conocimiento. AGESIC. "Plan Estratégico". Disponible en: https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/institucional/plan-estrategico. Consultada: abril, 2019

Presidencia de la República (s.f.c) Agencia de Gobierno Electrónico y Sociedad de la Información y el Conocimiento. AGESIC. "División Centro de Operaciones de Ciberseguridad (SOC). Disponible en: (https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/institucional/estructura-del-organismo/division-centro-operaciones-ciberseguridad-soc). Consultada: agosto, 2019

Presidencia de la República (2018) Agencia de Gobierno Electrónico y Sociedad de la Información y el Conocimiento. AGESIC. "Marco de Ciberseguridad". Disponible en: https://archivos.agesic.gub.uy/nextcloud/index.php/s/cgbssgiLEopFcRm#pdfviewer. Consultada: mayo, 2019

Presidencia de la República (mayo, 2019) "Agenda Uruguay Digital 2020. Transformación con equidad". Disponible en: https://uruguaydigital.uy/wps/wcm/connect/urudigital/6bd54ea6-1207-4cfa-bafb-c859bdac8019/Descargar+Agenda+Uruguay+Digital+2020.pdf?MOD=AJPERES&CONVERT_TO=url&CACHEID=6bd54ea6-1207-4cfa-bafb-c859bdac8019. Consultada, julio 2019

Presidencia de la República (2019) Agencia de Gobierno Electrónico y Sociedad de la Información y el Conocimiento. AGESIC. "Uruguay: Gobierno Digital y D9". Disponible en: https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/uruguay-gobierno-digital-d9. Consultada: mayo, 2019

Olavarría Gambi, M. (2007) "Conceptos básicos en el análisis de políticas públicas", en: *Documentos de Trabajo,* n.º 11, INAP, Universidad de Chile

Sabiguero, A., Nieves, M., Ibarra, V., Jackson, M., Messano, F., Esnal, G. (juldic.,2016). Relaciones entre soberanía y tecnología en los tiempos de Internet. *Revista de la Facultad de Derecho*, (41), DOI: http://dx.doi.org/10.22187/rfd2016211. pp. 259-286.

United Nations (2018) “2018 UN E-Government Survey”. Disponible en: (https://publicadministration.un.org/egovkb/en-us/Resources/E-Government-Survey-in-Media/ID/1901/Uruguay-es-l237der-en-Am233rica-Latina-y-el-Caribe-con-el-gobierno-digital-m225s-avanzado). Consultada: julio, 2019

Verdes-Montenegro Escánez, F. (2013) “La Teoría del Poder Estructural y la Securitización: Una Propuesta Teórica para el Estudio de las Transformaciones del Poder y la Seguridad”.[Work in progress]. Universidad Complutense de Madrid. Disponible en: https://aecpa.es/es-es/la-teoria-del-poder-estructural-y-la-securitizacion-una-propuesta-teo/congress-papers/574/. Consultada en: diciembre, 2019

Wæver, O. (1998) “Securitization and Desecuritization”, en: Ronnie D. Lipschutz (Ed.), *On Security.* New York: Columbia University Press