Facultad Latinoamericana de Ciencias Sociales, FLACSO Ecuador
Departamento de Estudios Internacionales y Comunicación
Convocatoria 2016-2018

Tesis para obtener el título de maestría de investigación en Relaciones Internacionales con mención en Seguridad y Derechos Humanos

La construcción de seguridad cibernética de Ecuador y Uruguay

Christian Santiago Santander Jiménez

Asesor: Daniel Pontón
Lectores: Johanna Espín y Pablo Medina Pérez

Quito, enero de 2019

Para Christian y Paulina, ustedes me enseñaron el valor de la constancia.

Para Daniela, porque me pediste estar en esta dedicatoria, pero especialmente, por tu apoyo incondicional.

Tabla de contenidos

Ilustraciones

Gráficos

Tablas

Declaración de cesión de derecho de publicación de la tesis

Yo, Christian Santiago Santander Jiménez, autor de la tesis titulada *La construcción de seguridad cibernética de Ecuador y Uruguay* declaro que la obra es de mi exclusiva autoría, que la he elaborado para obtener el título de maestría de investigación en Relaciones Internacionales con mención en Seguridad y Derechos Humanos concedido por la Facultad Latinoamericana de Ciencias Sociales, FLACSO Ecuador.

Cedo a la FLACSO Ecuador los derechos exclusivos de reproducción, comunicación pública, distribución y divulgación, bajo la licencia Creative Commones 3.0 Ecuador (CC BY-NC-ND 3.0 EC), para que esta universidad la publique en su repositorio institucional, siempre y cuando el objetivo no sea obtener un beneficio económico.

Quito, enero de 2019

Santiago Santander Jiménez

Resumen

La actual configuración del orden internacional y el comportamiento de los actores que lo conforman han promovido nuevas temáticas de estudio de interés para las Relaciones Internacionales, la seguridad y los derechos humanos. Los adelantos tecnológicos y la rápida expansión del Internet construyeron un escenario cibernético en el que existen amenazas y riesgos para quien interactúa en él. Esta realidad no es ajena a América del Sur. Los países que la conforman deben emprender medidas de seguridad cibernética que mitiguen el amplio alcance de las amenazas y su gran diversidad de fuentes.

Si bien las agendas de seguridad cibernética son necesarias en todos los países de la región, en la práctica, existen importantes brechas en sus procesos de construcción. Ecuador y Uruguay son países con características similares, pero que, en términos de seguridad cibernética son diferentes. Si bien Ecuador estaría enfrentando 2,5 veces más ataques que la mayoría de los países de la región, no ha desarrollado una agenda de seguridad cibernética en la misma medida que Uruguay, país pionero de América del Sur en temas de ciberseguridad. Esta investigación explica la brecha entre los dos países al responder ¿Cómo se diferencian los factores del proceso de securitización en la construcción de la agenda de seguridad cibernética de Ecuador en comparación con Uruguay entre el 2007 y 2017?

Para ello, se establece la importancia de los elementos conceptuales que aporta la teoría de la securitización en la construcción de agendas de seguridad cibernética como resultado de procesos intersubjetivos que permiten la materialización de prácticas concretas. Considerando las dimensiones conceptuales propuestas por Buzan y aquellas propuestas por Balzacq, los elementos de securitización pueden ser clasificados en factores internos y factores externos. Como factores internos: el objeto referente, la audiencia y el actor securitizador; y, como factores externos: el contexto, las relaciones de poder y las prácticas e instrumentos. Estos factores son analizados en los casos empíricos, Ecuador y Uruguay, para posteriormente ser comparados a través del método de la diferencia de Stuart Mill.

Se concluye que la agenda de seguridad cibernética de Ecuador tiene un menor desarrollo en comparación con la de Uruguay debido al alcance del objeto referente, influenciado en gran medida por el contexto, y la audiencia a la que se destina el discurso securitizador para la

construcción de las agendas de seguridad cibernética y materialización de prácticas determinadas.

Abstract

The current configuration of the international order and the behavior of the actors that comprise it, have promoted new topics of study of interest in International Relations, security and human rights. The technological advances and the rapid expansion of the Internet had built a cyber-scenario with threats and risks for those who interact in it. This reality is not strange to South America. The countries that include it, must take on cybersecurity measures that mitigate the wide range of threats and the great diversity of sources.

Despite the need of all the countries in the region for cybersecurity agendas, in practice, there are important gaps in their construction processes. Ecuador and Uruguay are countries with similar characteristics, but which, in terms of cybersecurity, are different. Even though, Ecuador faces 2.5 times more attacks than most countries in the region, it has not developed a cybersecurity agenda to the same extent as Uruguay, which is the first country in South America in terms of cybersecurity. This research explains the gap between the two countries answering how does the process of construction of Ecuador's cybersecurity agenda differ from Uruguay's cybersecurity agenda construction, between 2007 and 2017?

For that purpose, is important to establish the conceptual elements provided by the theory of securitization for the construction of cybersecurity agendas as a result of inter subjective processes that allow the embodiment of concrete practices. Considering the conceptual dimensions proposed by Buzan and those proposed by Balzacq, the elements of securitization can be classified into: internal factors and external factors. As internal factors: the reference object, the audience and the securitizing actor. And, as external factors: the context, power relations and practices and instruments. These factors are analyzed in the empirical cases, Ecuador and Uruguay, to be later compared through the method of difference proposed by Stuart Mill.

It is concluded that the cybersecurity agenda of Ecuador has a lesser development compared to Uruguay, due to the scope of the reference object, influenced to a large extent by the context, and the audience to which the securitizing speech is intended for the construction of cybersecurity agendas and materialization of certain practices.

Agradecimientos

A la Facultad Latinoamericana de Ciencias Sociales, FLACSO – Ecuador, a su cuerpo docente y personal administrativo por una experiencia académica de la más alta calidad.

A los amigos que compartieron conmigo durante el arduo camino de la maestría experiencias, reflexiones, madrugadas, risas y muchos mensajes.

A mi familia, quienes siempre me alientan a dar un paso más, a emprender un nuevo reto, a perseguir un nuevo sueño.

Introducción

El desarrollo tecnológico, la rápida expansión del Internet y el perfeccionamiento de las Tecnologías de la Información y la Comunicación (TICs), promovieron la creación de un nuevo espacio de interacción social y estatal cuyos cimientos están conformados por la relación entre la computación y las redes. Este nuevo espacio cibernético se ha convertido en una prioridad de seguridad nacional de la mayoría de los países del mundo. El ciberespacio aporta con herramientas que sirven como nuevos mecanismos para el cometimiento de actos ilícitos o delictivos, generado importantes amenazas a la seguridad estatal. El Sistema Internacional y los países que lo integran han sido, por varias ocasiones, testigos de ataques a la seguridad de un Estado a través de medios cibernéticos. Los casos más conocidos a nivel internacional son: la denegación de servicios de Rusia a Estonia, el ataque a través de Stunex en contra de instalaciones nucleares iraníes y las filtraciones a la Agencia de Seguridad Nacional de Estados Unidos (Lewis 2014).

Varias investigaciones realizadas por organismos internacionales como la Organización de Estados Americanos o la Organización de las Naciones Unidas exponen el preocupante crecimiento del numérico de ataques cibernéticos que tienen como objetivo afectar a la infraestructura crítica[1] de un Estado. Los ataques son efectuados por criminales que buscan obtener réditos económicos o por individuos con agendas políticas propias y contrarias a gobiernos o instituciones privadas (OEA 2015).

La Organización de las Naciones Unidas ha visibilizado el amplio alcance que tiene un ataque de naturaleza cibernética. Para este organismo,

> las amenazas reales y potenciales en la esfera de la seguridad de la información constituyen algunos de los problemas más graves del siglo XXI. Las amenazas derivan de una amplia gama de fuentes y se manifiestan como actividades desestabilizadoras dirigidas por igual contra particulares, empresas, elementos de la infraestructura nacional y gobiernos. Sus efectos entrañan considerables riesgos para la seguridad pública, la seguridad de las naciones y la estabilidad de la comunidad internacional en su conjunto (ONU 2010).

[1] Caro Bejaramo (2011) define a la infraestructura crítica como el conjunto de infraestructuras "necesarias para el funcionamiento normal de los servicios básicos y los sistemas de producción de cualquier sociedad"

Ahora bien, se puede constatar que las amenazas y las vulnerabilidades sociales y estatales de naturaleza cibernética no son casos aislados. Los países con el más rápido e importante crecimiento tecnológico se han convertido en los países de origen de la mayor cantidad de ataques cibernéticos en el mundo. Sus capacidades han permitido, a actores públicos y privados, hacer uso de sus ventajas relativas para afectar a la seguridad cibernética de países con menor desarrollo en este ámbito. Entre la lista de países desde donde se originan los ataques cibernéticos se encuentran, Estados Unidos, Francia, Rusia, China y Argentina. Estos países son claramente diferentes en aspectos sociales, económicos o culturales; sin embargo, han considerado esencial el desarrollo de acciones de seguridad activas y reactivas en el dominio cibernético (Medina 2016). Estos países han promovido la creación y aplicación de una agenda de seguridad cibernética como mecanismo que permita hacer frente a las amenazas provenientes del uso de las redes, el Internet y de las Tecnologías de la Información y la Comunicación (TICs).

De igual forma, la complejidad inmersa en un ataque cibernético a la seguridad nacional hace necesaria la compresión de aquello que engloba el espacio cibernético.

1. Seguridad cibernética en América del Sur

Diversas posiciones teóricas permiten explicar el comportamiento de los actores internacionales frente amenazas a la seguridad cibernética. Por lo tanto, facultan centrar la atención en casos de estudio que, a partir de una investigación direccionada al carácter cualitativo, buscan comprender y explicar cómo se construyeron las agendas de seguridad cibernética en dos países de América del Sur. Para llegar a esta instancia, es necesario identificar los factores del proceso de securitización, como actores nacionales e internacionales y sus intereses en las agendas de seguridad estatales, a partir de sus percepciones de amenaza cibernética. Todos estos factores son identificados como partes integrantes del discurso de los actores relacionados a la agenda de ciberseguridad de un país y la materialización de dicho discurso en ciertas prácticas e instrumentos específicos.

Varios autores han empleado estas perspectivas para explicar el comportamiento del Estado frente a las amenazas cibernéticas. Brúculo y Venczel (2012), Quintero (2014) o Ibarra y Nieves (2016) se han enfocado en el análisis de la seguridad cibernética desde un nivel de análisis específico, enfocado primordialmente en Latinoamérica. Los dos primeros trabajos se han orientado al Consejo de Defensa Suramericano y a las políticas de la UNASUR en

relación con las amenazas cibernéticas a las que se enfrentan los países que integran estos organismos. Ibarra y Nieves (2016) realizan el análisis sobre la Organización de Estados Americanos con un enfoque de protección contra el terrorismo. Otros académicos como Jaramillo y Ucciferri (2016) y Leiva (2015) han centrado sus investigaciones sobre la seguridad cibernética en ciertos países de América del Sur, como Chile y Argentina.

Por otro lado, la interdependencia en términos tecnológicos y de conectividad de los países de la región, incrementa la vulnerabilidad de los Estados frente a las amenazas cibernéticas, creando una especie de efecto dominó. Es por este motivo que la promoción de cooperación entre entidades gubernamentales, sociedad e instituciones internacionales, que busca instaurar un espacio cibernético seguro, influye en las agendas de seguridad de la región (Carlini 2016). La importancia de la seguridad regional ha impulsado literatura centrada en los países de América del Sur y Ecuador. Sin embargo, se ha enfocado en amenazas a la seguridad estatal con mayor perceptibilidad social, como el narcotráfico, la trata o tráfico de personas e incluso el terrorismo. Si bien estos temas continuarán siendo de importancia para la investigación académica, no podemos olvidar otras áreas de la seguridad estatal. El espacio cibernético se ha convertido en un nuevo escenario para el cometimiento de delitos y un nuevo dominio de conflicto internacional; por lo tanto, es esencial generar aportes en otras áreas de la seguridad nacional. Esto permitiría evitar las afectaciones al espacio cibernético, generadas por amenazas que ocasionan importantes repercusiones al Estado, a sus instituciones y a la población civil en general.

La carencia de academia producida desde América del Sur sobre la seguridad cibernética impulsa el estudio de la agenda de seguridad cibernética de países de América del Sur con el fin de entender cómo estos países han protegido sus intereses nacionales y han buscado garantizar la seguridad de los ciudadanos. La importancia de las estrategias y planes de seguridad cibernética los convierten en mecanismos fundamentales para la prevención, tratamiento y solución de cualquier afectación generada por medio del espacio cibernético. Estas estrategias buscan enfrentar amenazas de seguridad cibernética, las cuales pueden materializarse en afectaciones a la sociedad civil, a las instituciones públicas y privadas, al medioambiente e incluso a la economía. Es por este motivo que la presente investigación tiene como objetivo explicar la diferencia de los factores de securitización en el proceso de construcción de la agenda de seguridad cibernética de Ecuador en comparación con Uruguay

entre 2007 y 2017 para aportar en la comprensión del establecimiento de políticas de seguridad cibernéticas en América Latina.

El Ecuador es un caso de estudio relevante de América del Sur al ocupar el tercer lugar de los países que se enfrentan a la mayor cantidad de ataques cibernéticos en un año. Las estadísticas revelan que, durante el 2016, el margen de ataques al Ecuador fue de 1,44% frente al promedio de la región, que fue desde 0,4% y 0,6% (Medina 2016). Es decir que, Ecuador se estaría enfrentado a 2,5 veces más ataques que la mayoría de los países de la región. Además, si bien Ecuador no cuenta con una estrategia nacional específica de seguridad cibernética, ha tenido importantes avances para el fortalecimiento de sus capacidades de seguridad frente a amenazas cibernéticas. Las evidencias de esta importante innovación son el Plan Nacional de Seguridad Integral del período 2011 – 2013 y del período 2014 – 2017, con sus respectivas agendas sectoriales. Por otro lado, decisiones de política exterior como aceptar la petición de asilo de Julian Assange, influenció a la seguridad cibernética. A partir del ingreso de Assange a la embajada de Ecuador en Londres, el 19 de junio de 2012 (El Universo 2012), el país ha sido objeto de un crecimiento de ataques cibernéticos.

Uruguay, por otro lado, es un caso relevante de estudio de América del Sur al ocupar el primer lugar de la región en el Índice Global de Ciberseguridad[2] y el puesto 29 a nivel mundial (International Telecommunication Union 2017). Este país ha demostrado un importante desarrollo en el ámbito de seguridad cibernética. En la actualidad "es el líder regional en el desarrollo de software de seguridad y un mercado de nuevas tecnologías y seguro contra la delincuencia cibernética" (BID y OEA 2016). Uruguay, al igual que Ecuador, no ha desarrollado una estrategia específica de seguridad cibernética. Sin embargo, la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento está ejecutando iniciativas de seguridad y confianza en el uso de las TICs (AGESIC 2017).

Las disparidades entre Ecuador y Uruguay en relación con las respuestas estatales frente a las amenazas cibernéticas impulsan el estudio de los dos países dentro de la región. Por un lado, Ecuador como país receptor de ataques cibernéticos con poco desarrollo de estrategias de

[2] Indicador de la Unión Internacional de Telecomunicación que mide cinco aspectos del país a través de 25 indicadores. Los aspectos de medición son: legal, técnico, organizacional, creación de capacidad y cooperación.

seguridad cibernética. Y, por otro lado, Uruguay, como el país líder en la región en seguridad cibernética.

Si bien la presente investigación no tiene una perspectiva completamente técnica de las amenazas, riegos y herramientas de seguridad cibernética, el proceso investigativo daría como resultado una visión de carácter académico sobre la agenda de seguridad cibernética desde los casos de Ecuador y Uruguay. Este aporte conformaría uno de los pocos, casi inexistentes, trabajos académicos de seguridad cibernética del país y de la región, con una perspectiva política basada en las Relaciones Internacionales y el proceso de securitización. Esta investigación cubriría un vacío académico del país en temas de seguridad, enfocándose en la construcción de seguridad a partir de amenazas que proyectan un constante crecimiento y desarrollo, elevando aún más la necesidad de preparar insumos que permitan acoplar las respuestas de los estados a dichas amenazas.

Es por estas disparidades que la presente investigación plantea como pregunta central ¿Cómo se diferencian los factores del proceso de securitización en la construcción de la agenda de seguridad cibernética de Ecuador en comparación con Uruguay entre el 2007 y 2017? El tiempo de estudio se basa en la instauración de un nuevo gobierno en el Ecuador en el 2007 y su permanencia en la administración del Estado hasta el 2017; así como, la fundación de la Agencias de Gobierno Electrónico y Sociedad de Información y Comunicación durante el 2007, una de los principales actores de ciberseguridad de Uruguay. El argumento central de esta tesis propone que la agenda de seguridad cibernética de Ecuador tiene un menor desarrollo en comparación con la de Uruguay debido a un menor adelanto o influencia de los factores internos y externos del proceso de securitización del espacio cibernético para la construcción de agendas entre el 2007 y 2017.

2. Soberanía digital y sus amenazas

El uso de Internet y de las redes a nivel mundial ha creado la necesidad de ampliar el concepto de soberanía para incluir al ámbito digital. En el ámbito de las Relaciones Internacionales, este nuevo entendimiento de soberanía permite la disolución de fronteras territoriales y la adaptación del concepto tradicional de orden westfaliano de soberanía al espacio cibernético. La soberanía digital se enfoca en la autonomía y autogestión del espacio cibernético conformado por los elementos tecnológicos de un Estado. Sin embargo, el espacio cibernético puede ser considerado fácilmente como un escenario de propiedad global. Esto se

debe a la interdependencia de redes e infraestructura de la información, incluyendo el Internet, las telecomunicaciones, los sistemas computacionales, los procesadores y controladores.

La soberanía digital y el espacio cibernético son considerados como los principales blancos de las amenazas cibernéticas. Los autores que han estudiado este aspecto de la seguridad nacional han presentado diferentes definiciones de amenaza, que en su gran mayoría dependen de las afectaciones de un ataque cibernético. Si bien este debate conceptual será abordado posteriormente, se debe resaltar que la presente investigación considera que la definición de Ullman (1983) aporta con los elementos conceptuales necesarios para esclarecer lo que representa una amenaza cibernética. Este autor propone un concepto mucho más amplio, en el que se comprende a la seguridad cibernética como aquella que tiene la capacidad inmediata de perturbar la calidad de vida de la población y limitar las decisiones de un organismo estatal.

Las posiciones teóricas clásicas de las Relaciones Internacionales han impulsado sus propias concepciones de seguridad cibernética. El realismo continúa con el enfoque en el Estado como actor unitario que se desenvuelve en un escenario internacional anárquico. Para los realistas, la seguridad cibernética es un mecanismo de defensa militar, de los intereses soberanos y de la sobrevivencia del Estado. La corriente liberal, por su parte, considera otro tipo de actores que pueden ejercer un rol importante en el ámbito de la seguridad. Para el liberalismo es fundamental la protección del Estado y la garantía de derechos individuales; por lo tanto, promueve la paz y la cooperación internacional. Si bien estas dos posiciones teóricas tienen fortalezas, la universalidad de sus presupuestos no logran abarcar los elementos necesarios para el estudio de la construcción de agendas de seguridad en países de América del Sur, como Ecuador y Uruguay. Debido a las limitaciones que presentan dichas teorías, esta investigación considera al constructivismo como el acercamiento teórico más adecuado para el estudio del tema aquí propuesto.

Una perspectiva de carácter constructivista permite comprender la construcción de agendas de seguridad en países que, en búsqueda de una respuesta a sus amenazas, establecen mecanismos que les permitan reducir sus vulnerabilidades cibernéticas. Su apertura teórica permite abordar una gran variedad de percepciones de amenaza a la seguridad. Además, a partir de las condiciones e intereses de actores, quienes proponen un conjunto de ideas,

conceptos, imágenes, creencias, valores, normas e instituciones; se puede conocer la percepción de seguridad cibernética a nivel nacional e internacional.

En este sentido, la teoría de la securitización es un instrumento que permite observar la construcción de políticas de seguridad cibernética a través de la securitización de la amenaza por medio del discurso y su aplicación. Para la Escuela de Copenhague, pionera en la teoría de la securitización,

> el entendimiento [de la Escuela de Copenhague] de la seguridad como una modalidad discursiva con una estructura retorica particular y un efecto político la hace particularmente apropiada para el estudio de la formación y evolución del discurso de seguridad cibernética (Hansen y Nissenbaum 2009).

La gran variedad de objetos referentes, de actores securitizadores y las múltiples amenazas al espacio cibernético, complejizan el marco teórico que permite la comprensión de las implicaciones políticas, normativas y discursivas en temas de seguridad cibernética (Deibert 2002). Sin embargo, la securitización del ámbito cibernético fusiona diferentes objetos referentes, especialmente aquellos que no se relacionan directamente con la colectividad. A través de la primera condición facilitadora propuesta por (Buzan, Waever y de Wilde 1998) sobre el aspecto interno del discurso, el cual debe seguir las condiciones gramaticales de la seguridad, se busca la interacción de diferentes tipos de lenguaje y reglas que expongan la necesidad de securitizar el espacio cibernético. En este sentido, para la securitización de este escenario existen tres modalidades, la hipersecuritización, prácticas diarias de seguridad y la tecnificación. La interacción de estas tres modalidades es notable en el espacio cibernético, y les brindan un carácter distintivo frente a otros ámbitos de la seguridad de un Estado (Hansen y Nissenbaum 2009).

Posiciones teóricas que parten desde la Escuela de Copenhague y la teoría de la securitización han impulsado nuevos elementos de análisis que se enfocan en condiciones más tangibles de la securitización. Balzacq, Léonard y Ruzicka (2015) parten desde el aspecto discursivo de Buzan, Waever y de Wilde para consolidar cuatro factores que se involucran en el proceso securitizador. Estos factores son: la audiencia, el contexto, las relaciones de poder y las práctica e instrumentos. Por su capacidad analitica y abarcativa, estos factores fueron analizados junto con aquellos propuestos por la Escuela de Copenhague. Además, se los ha

calsificado en factores internos y externos de la securitización. Los primeros se refieren al objeto referente, a la audiencia, al actor securitizador y su discurso. Mientras que los segundos, los factores externos, se refieren al contexto, a las relaciones de poder y a las prácticas e instrumentos. Todos estos factores son analizados en los casos de estudio que aborda esta investigación.

3. Un estudio comparado

Durante el desarrollo de la investigación, se observan las características de los factores internos y externos previamente mencionados en cada uno de los casos de estudio, estos son, Ecuador y Uruguay. Por medio de herramientas de investigación, que permitieron la obtención de resultados, se recolectó información de cada uno de los factores, a través de búsqueda documental de fuentes primarias y secundarias, documentos oficiales gubernamentales, legislación interna e internacional y búsqueda en internet. Una vez recopilada y triangulada la información empírica necesaria, se compararon los factores para encontrar las diferencias entre los casos de estudio.

Al optar por un estudio comparativo, se pueden identificar los factores que determinarían un contexto diferente de seguridad cibernética entre Ecuador y Uruguay. Es importante resaltar, nuevamente, que la selección de los dos países latinoamericanos no solo responde a sus semejanzas por ser Estados pequeños, también responde a la necesidad del método de contar con casos símiles en los que se enfaticen las diferencias que permitan responder a la pregunta de investigación. En este sentido, las similitudes entre los casos de estudio permiten acercarnos a los parámetros establecidos por John Stuart Mill para emplear el método de la diferencia en el ámbito de la seguridad cibernética como un recurso de comparación que explique las divergencias entre los factores internos y externos del discurso securitizador.

> Si en un caso en el que ocurre el fenómeno bajo investigación, y en un instante en el que no ocurre, tenemos todas las circunstancias en común salvo una, la que ocurre solo en la primera; la circunstancia por la cual las dos instancias difieren es el efecto, o la causa, o una parte indispensable del caso, del fenómeno (Mill 2009, 483).

Los casos de estudios seleccionados presentan características generales similares que permiten una comparación de los factores del proceso securitizador. Tanto Ecuador como

Uruguay son países relativamente pequeños en relación con los otros países de la región. Ecuador tiene una extensión territorial de 256 370 km2 con una población de 16 624 858 habitantes. Uruguay, por su lado, tiene una extensión territorial de 176 220 km2 y una población de 3 456 750 habitantes. Si bien Uruguay tiene un Producto Interno Bruto (PIB) per cápita considerablemente mayor durante el 2017, el crecimiento del PIB en los dos países es de aproximadamente el 2,5%. En temas de seguridad y defensa, el porcentaje del PIB destinado a los gastos en este ámbito durante el 2017 fue de 1,75% aproximadamente en los dos países (CIA 2018).

Es así como, la presente investigación inicia con una profundización del marco teórico, el cual hace énfasis en los debates conceptuales relacionados al espacio cibernético, la construcción social y la teoría de la securitización. El segundo capítulo explica los factores internos del proceso de securitización del espacio cibernético, primero de Uruguay y posteriormente de Ecuador. El tercer capítulo abarca los factores externos del discurso en los dos países de análisis. Tanto en el segundo como tercer capítulo se presentan, a manera de conclusión, las semejanzas y diferencias de los factores que han sido analizados en cada capítulo y el resultado de la aplicación del método de la diferencia. Por último, en el cuarto capítulo se presentan las conclusiones de la investigación, con un enfoque en los procesos de securitización de Ecuador y Uruguay. En este último capítulo se podrán identificar las principales limitaciones de la construcción de una agenda de seguridad cibernética ecuatoriana en relación con Uruguay, un país de características similares.

Capítulo 1

La seguridad cibernética como constructo social

Las diferentes corrientes teóricas de las Relaciones Internacionales y su capacidad explicativa de la realidad mundial permiten entender la seguridad cibernética desde una posición epistemológica particular. Cada una de ellas ha presentado su concepción de amenaza cibernética y como responder a ella.

El concepto seguridad se ha alineado al desarrollo de las principales posiciones teóricas de las Relaciones Internacionales. Es así como, iniciando desde una postura realista y neorrealista, la seguridad gira en torno al Estado como actor unitario. Para esta perspectiva, el Estado tiene el monopolio sobre el uso de la fuerza, a través del cual logra satisfacer sus intereses y garantizar su soberanía o sobrevivencia en un sistema anárquico (Velásquez y González 2014). La fuerza tiene una relación directa con el poder en términos materiales; por lo tanto, las medidas de carácter racional del Estado estarán direccionadas a la búsqueda del poder y, como consecuencia, a la seguridad en términos militares (Morgenthau 1986). El desbalance de poder en el sistema provee mayor seguridad para unos y menor para otros. “Los más poderosos disfrutan de mayores márgenes de seguridad al tratar con los menos poderosos” (Waltz 1988, 283).

Para estas corrientes teóricas, el espacio cibernético se convierte en un nuevo escenario internacional de interacción interestatal anárquica que tiene como objetivo primordial la búsqueda de poder. Por lo tanto, la seguridad cibernética es un mecanismo de defensa frente a los posibles ataques cibernéticos del enemigo. Para asegurar el espacio cibernético, desde una posición militar, los estados, “a nivel global, están construyendo sistemas de defensa cibernética e incluyen escenarios de ataques cibernéticos en sus planes estratégicos” (Kremer 2014, 230). El Realismo considera que el objetivo de la amenaza son la soberanía e integridad del Estado como actor unitario. Si bien “alguna de la tecnología es nueva, así como la capacidad global de ingeniosos adversarios digitales; las nociones básicas de ataque y defensa de información y de sistemas de información son tan viejas como la guerra en sí” (Erikson y Giacomello 2006, 229).

Por otro lado, para el liberalismo y el neoliberalismo, como otras categorías teóricas de las Relaciones Internacionales, la seguridad se enfoca en el establecimiento de paz mediante

reglas y direcciones establecidas por diversos actores internacionales. Para estas perspectivas, la cooperación elimina el conflicto y la inseguridad como resultado de acciones estatales (Reus-Smit 2005). Para la seguridad, en términos liberales, es fundamental el rol de las organizaciones internacionales, las normas, reglamentos y regímenes (Grocio 1925) (Karns y Mingst 2004). En esta línea, Kant (1975) propone seis principios para alcanzar la paz perpetua[3]. Mientras otros pensadores fundamentan que la interdependencia compleja entre una gran variedad de actores asimétricos en diversas temáticas fomenta la seguridad del sistema y de sus actores (Keohane y Nye 1988).

El liberalismo considera a la seguridad cibernética no solo como el mecanismo de protección del Estado, sino también como el mecanismo de protección a los derechos individuales. Para esta posición teórica "el fin último no es primordialmente la preservación y protección de la integridad y soberanía estatal, sino la integridad del individuo" (Kremer 2014, 232). Por lo tanto, la seguridad cibernética busca mitigar las amenazas a los derechos de los ciudadanos por parte de cualquier actor nacional e internacional. Para esta teoría los nuevos actores internacionales tienen un rol fundamental, positivo o negativo, en la seguridad cibernética.

> La aparición del Internet no solo hizo posible la comunicación global en tiempo real para las ONGs existentes, también lo hizo posible para nuevos y exclusivos grupos *online*. Esto, obviamente, puede tener efectos positivos y negativos: integración, cooperación y liberalización podrían ser facilitados, pero también el terrorismo, el crimen transnacional y la desestabilización de estados (Erikson y Giacomello 2006, 232).

Ahora bien, estas perspectivas teóricas y su concepción de seguridad se han enfrentado a varias críticas. Por un lado, las posiciones de seguridad alineadas a las tendencias realistas limitan, en gran medida, la inclusión de elementos que deberían ser considerados. El enfoque plenamente militar no permite explicar las afectaciones a la seguridad por parte de actores no estatales que mantienen diversas agendas. El realismo no sería suficiente para entender e ilustrar la seguridad en el sistema internacional (Keohane, Theory of World Politics:

[3] Los seis principios de la paz perpetua: 1) "ningún tratado de paz en el cuál esté tácitamente reservado un asunto para una guerra futura será válido"; 2) "ningún Estado independiente, grande o pequeño, será cedido a otro Estado por medio de herencia, intercambio, compra o donación"; 3) "los ejércitos permanentes deberán desaparecer por completo con el tiempo"; 4) "la deuda nacional de deberá ser contraída con el fin de ocasionar tensiones entre Estados"; 5) "ningún Estado debe inmiscuirse por la fuerza en la constitución o el gobierno de otro Estado" y 6) "ningún Estado debe, durante la guerra con otro Estado, permitir actos de hostilidad que imposibiliten la confianza mutua en la paz futura. Tales son, por ejemplo, el empleo de asesinos, envenenadores, el quebrantamiento de capitulaciones o el incitamiento a la traición" (Kant 1795)

Structural Realism and Beyond 1986). Por otro lado, en las tendencias liberales no se consideran, como elementos de análisis, las motivaciones que promueven ciertas realidades. Si bien es cierto que abarcan un mayor tipo de actores, su enfoque en la cooperación y la paz no permite una explicación centrada en seguridad, principalmente por medios materiales (Grieco 1988).

Si nos enfocamos específicamente en la seguridad cibernética, las posiciones teóricas realistas no logran adaptarse a los factores que influyen en el entendimiento de la seguridad en una era digital. El realismo se ve limitado a la comprensión de este fenómeno y abordaría "el reto de la revolución de la información casi de la misma manera que ha abordado previos retos de transnacionalización, interdependencia compleja y globalización" (Erikson y Giacomello 2006, 229). Por su parte, el liberalismo no permite un abordaje integral a la seguridad cibernética por su énfasis en aspectos positivos en lugar de vulnerabilidades y amenazas cibernéticas crecientes. Al igual que el realismo, el liberalismo considera que la seguridad cibernética responde a factores teóricos universales, lo que limita su análisis. Por lo tanto, la presente investigación se enfoca en una tercera tendencia de las Relaciones Internacionales, el Constructivismo.

Las agendas de seguridad cibernética de Ecuador y Uruguay son construidas a partir de procesos de securitización en los que se desarrollan factores determinados, especialmente, son el resultado de la interacción social entre diversos actores. Partiendo de esta premisa, la teoría Constructivista de las Relaciones Internacionales se configura como la macro teoría que enmarca la investigación de las agendas de seguridad en los casos de estudio. Además, la teoría de la securitización es el instrumento teórico que permite identificar los factores influyentes en el proceso de inclusión de una temática a las agendas de seguridad de los estados. La importancia de las capacidades analíticas con las que aportan estas teorías permite determinar los factores que influyen en la securitización del espacio cibernético en los países de América del Sur y, específicamente, en Ecuador y Uruguay. Por lo tanto, el presente capítulo abordara el debate teórico constructivista como punto de partida. Se continuará con el desarrollo de la teoría de la securitización y la securitización del espacio cibernético. Finalmente, se establecerán los factores a ser analizados y comparados en los casos de Ecuador y Uruguay.

1.1. Seguridad en las Relaciones Internacionales

La propuesta de una nueva forma de entender la realidad, una realidad basada en la interacción social y las ideas se genera en base al Constructivismo. Esta posición teórica de las Relaciones Internacionales nace a partir de la premisa de que todo tipo de acción humana o colectiva, incluyendo la seguridad, es el resultado de un conjunto de interacciones. Para esta posición teórica la realidad es construida de manera constante, no es estática. Por lo tanto, el conocimiento tampoco es estático y está en permanente construcción. En vista de la constante construcción y transformación de la realidad, las ideas son el pilar fundamental de análisis (Reus-Smit 2005).

Al dar prioridad a las ideas, se establece la necesidad de consolidar identidades que permitan fomentar una cultura de seguridad, construir nuevas ideas, valores e instituciones enfocadas en la disminución de los riesgos y amenazas de los actores internacionales involucrados en el sistema. Además, para uno de los mayores representantes de la teoría constructivista, Wendt (2004), las amenazas sociales que representarían una afectación a la seguridad son una construcción de interacciones entre actores que se transforman en estructuras con su permanencia en el tiempo. Para este pensador, los enfoques más tradicionales basados en supuestos realistas o liberales no permiten explicar adecuadamente el comportamiento de los Estados. Al tener un enfoque en las ideas, no solo es posible explicar el comportamiento de los actores, sino también la estructura en la que se desenvuelven.

El Constructivismo se diferencia de otras perspectivas teóricas de corte clásico debido a la participación primordial de cuatro factores: la alternativa al materialismo, la construcción de los intereses de Estado, la constitución mutua de estructura y agencia, y las múltiples lógicas de anarquía. Estos factores permiten que el Constructivismo aborde posiciones filosóficas y empíricas que no podrían enfocarse a través de modelos tradicionales como el materialismo realista o liberalista, y el racionalismo de los neorrealistas o neoliberalistas (Hurd 2008).

Como alternativa al materialismo, el Constructivismo propone el significado de un objeto o de una práctica como el resultado de construcciones sociales a partir de ideas, las cuales pueden cambiar con el tiempo. Las ideas forman la política y realidad internacional una vez que han alcanzado intersubjetividad entre diversos individuos y han sido institucionalizadas. Al contrario del realismo, “el Constructivismo sugiere que las fuerzas materiales deben ser entendidas a través de los conceptos que definen su significado para la vida humana” (Hurd

2008, 301). Además, el Constructivismo defiende la premisa de que los intereses nacionales son el resultado de una construcción social y que no están naturalmente establecidos. En este sentido, los intereses estatales se construyen debido a intereses e identidades de actores que se desenvuelven en un escenario interactivo. Sin embargo, la influencia no es unidireccional; el escenario o estructura y los actores o agencias se constituyen mutuamente[4]. Por último, para el constructivismo la anarquía no establece patrones de comportamiento basados en el conflicto o en la cooperación, sino que la anarquía es una construcción social (Hurd 2008; Bull 2002).

La seguridad, incluso la cibernética, es una construcción social de prácticas enfocadas en ideas e intereses específicos. Sin un escenario en el que la interacción entre los actores genere riesgos o amenazas, no cabría la necesidad de implementar una agenda de seguridad, ni de ejecutar procesos securitizadores. "Considere dos actores -ego y alter- se encuentran por primera vez. Cada uno quiere sobrevivir y tiene ciertas capacidades materiales, pero ninguno de los dos tiene obligaciones biológicas ni domesticas de búsqueda de poder, gloria o conquista, por lo tanto, no hay historia de seguridad e inseguridad entre los dos" (Wendt 1992, 404).

Una de las ventajas de este acercamiento teórico, es su aporte para el estudio de la cultura en las relaciones internacionales. El Constructivismo permite la creación de varias realidades como instituciones, reglas, normas y la forma en la que estas se comportan, mediante su fundamento en ideas e intereses. Este acercamiento permite considerar a la cultura como un elemento integral de las relaciones entre actores internacionales y las sociedades que lo conforman. De esta forma se incorpora una nueva visión que nos permite analizar los riesgos y amenazas que se presentan a través de contextos culturales y que, gracias al desarrollo tecnológico y la globalización, tienen un alcance mundial más amplio (Reus-Smit 2005).

Es fundamental resaltar el hecho de que para el Constructivismo la estructura internacional es un conjunto social de interacciones entre diferentes actores, pero que está determinada por la acción humana.

[4] Para Hurd (2008, 303) por estructura se refiere a "las instituciones y significados compartidos que componen el contexto de la acción internacional". Por agente se refiere a "cualquier entidad que opera como un actor en aquel contexto".

> gracias a las relaciones de identidad de los elementos del sistema es posible crear un tipo de seguridad colectiva capaz de preservar los intereses de los actores internacionales. Esto lleva a considerar, desde la visión del constructivismo, al referente central de la seguridad a la identidad ya sea de grupos, de colectividades o de instituciones que en el proceso de sus relaciones hayan constituido lazos infranqueables que determinan su posición y papel en el sistema (Orozco 2006).

Este principio será empleado posteriormente para el desarrollo de la teoría de la securitización de la Escuela de Copenhague.

1.2. Teorías de la securitización

A partir de una posición constructivista, que posteriormente incorpora elementos de poder y capacidad, se crea la teoría de la securitización como un proceso que permite incorporar en las agendas de seguridad fenómenos que anteriormente no eran considerados como problemas de esta naturaleza. Las diferentes perspectivas teóricas referentes a la securitización tienen como objetivo primordial comprender cómo y por qué determinados temas llegan a constituirse como problemas de seguridad de un Estado y cuáles son los efectos de este proceso.

La definición de securitización abarca diferentes elementos conceptuales que han sido definidos por Buzan, Waever y de Wilde (1998). Para estos autores “la exacta definición y criterio de securitización está constituida por el establecimiento intersubjetivo de una amenaza existencial con suficiente proyección como para tener efectos políticos substanciales” (Buzan, Waever y de Wilde 1998, 23). Para la teoría de la securitización, al igual que para el Constructivismo, la intersubjetividad se convierte en el elemento esencial para el posicionamiento de una idea formada socialmente. Únicamente cuando existe la intersubjetividad se logra materializar las ideas en prácticas concretas, en este caso, en políticas de seguridad (Sanahuja y Schünemann 2012).

Para la teoría de la securitización según Buzan, Waever y de Wilde (1998) las características especiales de una amenaza motivan la implementación de medidas extraordinarias que puedan hacerles frente. Se entiende, en este caso, como medidas extraordinarias a respuestas que se alejan de las decisiones de política pública convencionales. Los autores brindan como ejemplo limitaciones específicas a la ciudadanía que, en caso de no existir la amenaza, no se aplicarían. El proteccionismo o el desplegar a la policía o a los militares, son otros ejemplos

de medidas extraordinarias que podrían emplearse frente a una amenaza. En el espacio cibernético, podrían ser consideradas como medidas extraordinarias limitaciones al acceso de información o el control estatales de las telecomunicaciones.

En primer lugar, los objetos referentes son "las cosas que están existencialmente amenazadas y que tienen un legítimo reclamo de supervivencia" (Buzan, Waever y de Wilde 1998, 26). Uno de los principios de la teoría de la securitización, es la capacidad de los actores de convertir a cualquier elemento en un objeto referente. Sin embargo, es necesario resaltar que este objeto debe estar en la capacidad de legitimar la creación de una agenda de seguridad. Esta capacidad está dada por la importancia de su supervivencia en una sociedad. Si la supervivencia del objeto referente no es fundamental, no se logrará securitizar un fenómeno.

El actor securitizador puede conformarse por aquellos "actores que securitizan los problemas al declarar algo -un objeto referente- existencialmente amenazado" (Buzan, Waever y de Wilde 1998, 26). Pueden ejercer su rol de manera individual y colectiva, además, por lo general, son personas con la capacidad de que su discurso pueda ser difundido y que sea receptado por la audiencia. Los actores securitizadores más comunes son los políticos; sin embargo, también ejercen este rol: burócratas, gobiernos o grupos de presión. La autoridad de estos actores y su relación de poder con la audiencia, les permiten ejecutar de mejor manera el proceso securitizador y controlar sus resultados.

La audiencia, por su parte, es la sociedad que recibe el discurso securitizador. Su participación en el proceso es fundamental debido al rol que mantienen en la legitimación de la inclusión de un fenómeno en la agenda de seguridad. La audiencia es quien determina, en última instancia, que el objeto referente debe ser securitizado o no. La respuesta al discurso y al objeto referente se denota en Buzan, Waever y de Wilde (1998, 27) quienes exponen que "se hace más fácil si se puede apuntar a temas asociados con las amenazas, pero la última palabra de la securitización es social en lugar de técnica, y es entre el actor securitizador y su audiencia en referencia a algo que valoran".

Empleando los elementos propuestos en la Escuela de Copenhague por Buzan, Waever y de Wilde (1998), autores como Balzacq (2011) han definido a la securitización como

> un conjunto articulado de prácticas a través de las cuales los artefactos heurísticos (metáforas, herramientas de política, repertorios de imágenes, analogías, estereotipos, emociones, etc.) son movilizados contextualmente por un actor securitizador, quien trabaja para promover a una audiencia la construcción de una red coherente de implicaciones (sentimientos, sensaciones, pensamientos e intuiciones) sobre una vulnerabilidad critica de un objeto referente.

Las diferentes perceptivas teóricas sobre la securitización convergen, según Balzacq et. al. (2015), en cuatro dimensiones conceptuales: la audiencia, el contexto, las relaciones de poder y las prácticas e instrumentos. Estos cuatro conceptos influyen en la securitización de ciertos fenómenos y permiten explicar el éxito o alcance del proceso securitizador. Debido a su relevancia teórica, estos elementos deben ser abordados individualmente.

Audiencia

La importancia de la audiencia en las teorías de la securitización es manifestada por un proceso de intersubjetividad que requiere de aceptación. Buzan et. al. (1998, 23) consideran que "un problema es securitizado solo si, y cuando, una audiencia lo haya aceptado". La aceptación de la audiencia hace posible la legitimación de agendas de seguridad que ejecuten medidas especiales de respuesta al problema; medidas que no son consideradas en agendas políticas convencionales. Es por este motivo que las acciones de securitización buscan convencer a la audiencia de la necesidad de proteger al objeto referente de las amenazas latentes por medio de procedimientos extraordinarios.

Para las perspectivas de la teoría de la securitización, esta dimensión presenta complejidades especiales. La primera de las complejidades radica en la dificultad de establecer mecanismos que permitan determinar el nivel aceptación de la audiencia a la securitización de un fenómeno. Si bien es cierto que la ausencia de aceptación de la audiencia no permitiría el proceso de securitización, no se acordado una forma de identificar el nivel de aceptación de la audiencia. Esta complejidad de análisis se profundiza aún más cuando en el proceso de securitización participan más de una audiencia. Para Salter (2008) cada audiencia tiene características distinticas que afectan la aceptación, y por lo tanto el éxito, del proceso securitizador.

Relaciones de poder

Las relaciones de poder participan como elemento del proceso securitizador al otorgar a los diferentes actores (securitizador, sujeto referente o audiencias) la capacidad de influenciarse entre unos y otros. Esta dimensión conceptual ha tenido un rol protagónico en las teorías de la securitización; de manera especial, en los primeros debates sobre securitización. Estas perspectivas teóricas de carácter tradicional explicaban la capacidad de las elites de securitizar la agenda por ostentar mayor poder frente al resto de actores y su capacidad de securitizar como un mecanismo más de dominación. Waver (1995) establece que "por definición, algo es un problema de seguridad cuando las élites declaran que lo sea".

Por otro lado, con el desarrollo de la teoría de la securitización, se permite analizar una gran variad de relaciones de poder, no solo de las élites que ostentan poder en el sentido realista, sino también el poder de otros autores como la audiencia, quien está en capacidad de securitizar o no un fenómeno por medio de su aceptación. Así, las relaciones de poder permiten, o no, el éxito de los procesos de securitización.

Contexto

La importancia del contexto en la teoría de la securitización está dada por la capacidad que tiene está dimensión conceptual de modificar el proceso y los resultados de la securitización. Varios autores han desarrollado diferentes conceptos para referirse al contexto de un proceso securitizador. Para Buzan et. al. (1998) esta dimensión conceptual puede referirse a dos elementos diferentes. Por un lado, el contexto puede ser sinónimo de ámbito. Es decir que, se refiere a los espacios que se podrían securitizar como el político, militar, social, entre otros. Por otro lado, el contexto también puede referirse a todas las condiciones de carácter histórico que están relacionadas con la amenaza y que conforman sus características actuales.

Otro entendimiento sobre el concepto es propuesto por Wetherell (2001), quien realiza una diferenciación entre un contexto próximo y un contexto distante o externo. El contexto próximo "incluye las características inmediatas de la interacción" y el contexto distante comprende factores como "la clase social, la composición étnica de los participantes, las instituciones o sitios donde ocurre el discurso, y los escenarios ecológicos, regionales o culturales" (Whetherell 2001). Es decir que, el contexto próximo se refiere a las relaciones entre los actores y sus características y, el contexto distante, se refiere a condiciones externas

a la interacción entre los actores y que pueden estar previamente establecidas o son de carácter estructural.

Balzacq (2011), por su parte, argumenta que "el repertorio semántico de seguridad es una combinación de significados textuales, conocimientos del concepto adquirido a través del leguaje, escrito u oral, y el significado cultural, conocimiento histórico adquirido a través de interacciones previas y situaciones concurrentes". Estos elementos pueden ser enmarcados en la propuesta conceptual de Shegloff al clasificar a los significados textuales y concepto adquirido como características inmediatas de la interacción, es decir un contexto próximo. Por otro lado, el significado cultural y el conocimiento histórico pueden ser enmarcados en el contexto distante o externo.

Ahora bien, una vez que se han descrito los diferentes significados de contexto para la teoría de la securitización, es importante marcar el cuadro epistemológico de esta dimensión. El contexto puede ejercer un rol facilitador para la securitización de un fenómeno y servir de variable interviniente en el proceso (Buzan et. al. 1998). La importancia del contexto es destacada desde visiones internas y externas.

> La primera es aquella de la [escuela de Copenhague], donde el aspecto performativo de la seguridad cambia, por si misma, la configuración de un contexto. En contraste, la segunda visión considera que el contexto tiene un estado independiente, que le permite influenciar articulaciones de seguridad de una manera distintiva (Balzacq 2005).

Además, la visión externa permite considerar la influencia del contexto en el proceso de securitización, en el actor securitizador, en el sujeto referente y en la audiencia. Es decir que, por medio de esta visión, se le otorga al contexto la capacidad de generar las condiciones necesarias para la actuación de los actores involucrados en la securitización de un fenómeno. Es así como el contexto es, cada vez más, un elemento fundamental para comprender la incorporación de un tema en la agenda de seguridad de un país.

Prácticas e instrumentos

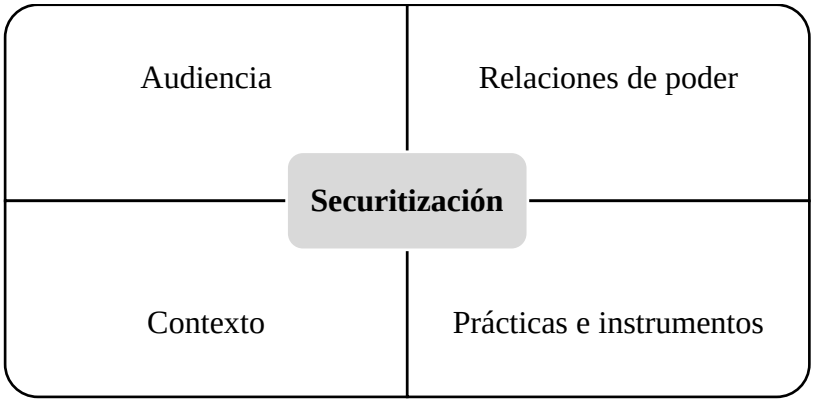
La teoría de la securitización nace a partir del ejercicio retórico o discursivo impulsado por la escuela de Copenhague, pero su evolución permite abarcar aspectos técnicos, prácticos e, incluso, capacidades materiales. La incorporación de este elemento a la teoría presenta un reto

importante, enfocado en la consolidación e interacción de un componente discursivo con un acercamiento práctico de la securitización. Los autores que defienden la importancia de un acercamiento práctico a la securitización suelen basarse en instrumentos o herramientas que son empleadas en los procesos de securitización. "Los instrumentos expresan una relación específica de seguridad. Ellos encarnan la mentalidad de agentes de seguridad y organizan interacciones" (Balzacq et. al. 2015).

Estas cuatro dimensiones conceptuales son resumidas por Balzacq (2015), quien menciona que:

> la teoría de la securitización se ha desarrollado considerablemente desde su formación original por parte de la [escuela de Copenhague]. Se ha dado atención significante al rol de la audiencia y a la importancia del aspecto intersubjetivo de la teoría. Estudiosos también han trabajado más en averiguar los efectos que tiene el contexto y el balance de poder entre actores tienen sobre los procesos securitizadores. Además, mientras la mayoría de la teoría solía enfocarse en la dirección de un acto discursivo verbal más explícito, […] la teoría se ha movido progresivamente hacia la investigación de prácticas con el fin de complementar o a veces transcender el énfasis inicial en enunciados lingüísticos.

Gráfico 1: Dimensiones conceptuales de la teoría de la securitización de Balzacq



Fuente: Balzacq et. al. 2015. 'Securitization' revisited: Theory and cases

"La teoría [de la securitización] se ha movido progresivamente hacia una investigación de prácticas con el fin de complementar o a veces trascender el énfasis inicial en enunciados lingüísticos" (Balzacq, Léonard y Ruzicka, 'Securitization' revisited: Theory and cases 2015). Las cuatro dimensiones conceptuales abordadas previamente se configuran en los factores que serán analizados en la construcción de agendas de seguridad cibernética de Ecuador y

Uruguay. Se han considerado estos factores debido a que abarcan los aspectos discursivos de la teoría de la securitización de la Escuela de Copenhague propuesta por Buzan, Waever y de Wilde (1998). Pero, además, las dimensiones conceptuales elegidas consideran factores que se enfocan en las prácticas de seguridad y en realidades institucionales que se encuentran alejadas del centro discursivo.

Por lo tanto, en base a lo propuesto por Buzan, Waever y de Wilde (1998) y lo propuesto por Balzacq (2015) los elementos que configuran la teoría de la securitización son de carácter interno o lingüístico y de carácter externo. El análisis de todos los elementos permite colocar el discurso en un contexto que afecta directamente a sus resultados. Todos los elementos propuestos por los pensadores previamente mencionados deben ser considerados en el proceso securitizador.

1.3. Securitización del espacio cibernético

La seguridad cibernética se enfoca en la contención de amenazas cibernéticas, las cuales pueden afectar a varios aspectos de la seguridad nacional. Estas amenazas son

> reales y potenciales en la esfera de la seguridad de la información […]. Las amenazas derivan de una amplia gama de fuentes y se manifiestan como actividades desestabilizadoras dirigidas por igual contra particulares, empresas, elementos de la infraestructura nacional y gobiernos. Sus efectos entrañan considerables riesgos para la seguridad pública, la seguridad de las naciones y la estabilidad de la comunidad internacional en su conjunto (ONU 2010).

Varios autores han desarrollado perspectivas teóricas basadas en la teoría de la securitización para observar como el ámbito cibernético es acoplado a la agenda de seguridad de un país. "Las nociones de amenazas cibernética se han originado tanto en la esfera privada como en la pública, entre actores militares, así como civiles" (Erikson y Giacomello 2006, 225). Además, la gran variedad de objetos referentes, de actores securitizadores y las múltiples amenazas complejizan el marco teórico que permitiría la comprensión de las implicaciones políticas, normativas y discursivas en temas de seguridad cibernética (Deibert 2002). Sin embargo, la securitización del espacio cibernético fusiona diferentes objetos referentes, especialmente aquellos que se relacionan directamente con la colectividad. A través de la primera condición facilitadora propuesta por (Buzan, Waever y de Wilde 1998) sobre el aspecto interno del

discurso que debe seguir las condiciones gramaticales de la seguridad, se busca la interacción de diferente lenguaje y reglas que expongan la necesidad de securitizar.

En este sentido, Bendrath, Eriksson y Giacomello (2007) van más allá de la tradicional teoría de la securitización propuesta por la Escuela de Copenhague y toman un modelo similar al propuesto por Balzacq. Ellos consideran que la seguridad en el ámbito cibernético debe, necesariamente, incorporar características, actores y condiciones del contexto para determinar la eficiencia de la securitización de la tecnología de la información. Por otro lado, Dunn Cavelty (2008) manifiesta que "las contramedidas que tienen lugar actualmente se basan en el análisis de riesgo y la administración de riesgo". Este autor toma el concepto de seguridad propuesto por Buzan y argumenta que la ausencia de medidas excepcionales en la agenda de los países para enfrentar amenazas de carácter cibernético son un ejemplo de securitización fallida.

La teoría de la securitización aplicada al espacio cibernético amplia la lógica tradicional de la amenaza y constituye una nueva en la que "dos nociones diferentes sobre seguridad se unen, la seguridad técnica y la seguridad nacional se convierten en una" (Cavelty 2008). De esta forma, los objetos referentes de la teoría de la securitización son la red y el individuo, los cuales están relacionados con el ámbito de la seguridad nacional.

Otras posiciones, como las de Hansen y Nissenbaum (2009), quienes mencionan que la securitización del espacio cibernético se da al:

> juntar objetos referentes, particularmente al proveer un enlace entre aquellos que no invocan de forma explícita una limitación colectiva, como 'red' o 'individuo', con aquellos que sí. Contestación y multi discursividad son, por lo tanto, encontradas en las articulaciones competitivas de objetos referentes enlazados; así como por el rastreo de potencial inestabilidad interna de cada discurso.

De esta forma, las autoras proponen una gramática específica que permite delinear tres modalidades de securitización en el espacio cibernético: hipersecuritización, prácticas de seguridad diaria y la tecnificación. La hipersecuritización se refiere a un proceso securitizador que sobrepasa a la amenaza. Para Hansen y Nissenbaum (2009), "el discurso de la seguridad cibernética depende de desastres cibernéticos multidimensionales que abarcan una larga lista

de severas amenazas en una monumental secuencia en cascada y el hecho de que ninguno de estos escenarios ha tenido lugar hasta ahora". La hipersecuritización se basa en el sobredimensionamiento de la amenaza y su proyección al futuro.

Las prácticas de seguridad diarias es la modalidad que se enfoca en la manera en que los actores securitizadores emplean experiencias individuales para buscar aceptación de medidas de seguridad en las redes y para hacer los escenarios de hipersecuritización más reales. Esta modalidad presenta características específicas enfocadas en el rol del individuo. Por un lado, puede ser un importante elemento para enfrentar las amenazas al objeto referente y, por otro, puede convertirse en una desventaja o, incluso, en una amenaza (Hansen y Nissenbaum 2009).

La tercera y última modalidad de la securitización del espacio cibernético propuesta por Hansen y Nissenbaum, es la tecnificación. En esta modalidad, expertos técnicos relacionados al espacio cibernético tienen un rol privilegiado y la capacidad de legitimar el discurso securitizador de otros actores en el proceso. Además, la participación de expertos permite despolitizar la inclusión de temas cibernéticos en la agenda de seguridad, por medio de un discurso racional y técnico. "Las tecnificaciones desempeñan un rol crucial en la legitimación de la securitización cibernética por sí mismas, así como un aporte a la hipersecuritización y a las conversaciones de la autoridad, para el público, acerca del significado de prácticas diarias" (Hansen y Nissenbaum 2009).

Es decir que, como parte del análisis de los factores del proceso de securitización en los dos casos sudamericanos, es necesario considerar la modalidad bajo la cual se desarrolla el aspecto discursivo de la securitización en el espacio cibernético. Esto permitirá demostrar si las estrategias de seguridad cibernética existentes en Ecuador y Uruguay se dieron a partir de hipersecuritización, prácticas de seguridad diaria o la tecnificación.

Para la securitización del espacio cibernético y la implementación de agendas enfocadas en este ámbito es necesario que la audiencia forme una percepción de amenaza cibernética. Para alcanzar una percepción nacional de amenaza es fundamental que los líderes políticos consideren el espacio cibernético y el Internet como escenarios propicios de nuevas amenazas. La percepción de amenaza por parte de estos actores específicos depende de factores como "el interés personal, la experiencia directa de una acción cibernética maliciosa, atención

mediática o la prominencia de seguridad cibernética en sus agendas nacionales e internacionales" (Lewis 2014, 566). La posición de estos actores securitizadores se ve reforzada con la transnacionalidad de la amenaza cibernética, la que provoca una activa participación de actores internacionales en la formación de percepción de amenaza cibernética, fortaleciendo el papel de los líderes políticos.

> Si la percepción de amenaza cibernética en muchos países es determinada por influencias exógenas, la más importante de estas influencias exógenas es la discusión internacional de amplio rango sobre amenazas cibernéticas que ha crecido en los últimos años, reorganizando las percepciones de amenaza y sus políticas (Lewis 2014, 568).

Capítulo 2
Factores internos del discurso securitizador

En el presente apartado se abordarán los factores internos relacionados al discurso securitizador del espacio cibernético en Uruguay y Ecuador. Los tres elementos internos del discurso securitizador son: el objeto referente, el actor securitizador y la audiencia (Buzan, Waever y de Wilde 1998). Se analizará a profundidad en términos empíricos, cada uno de ellos, en los dos países objeto de análisis.

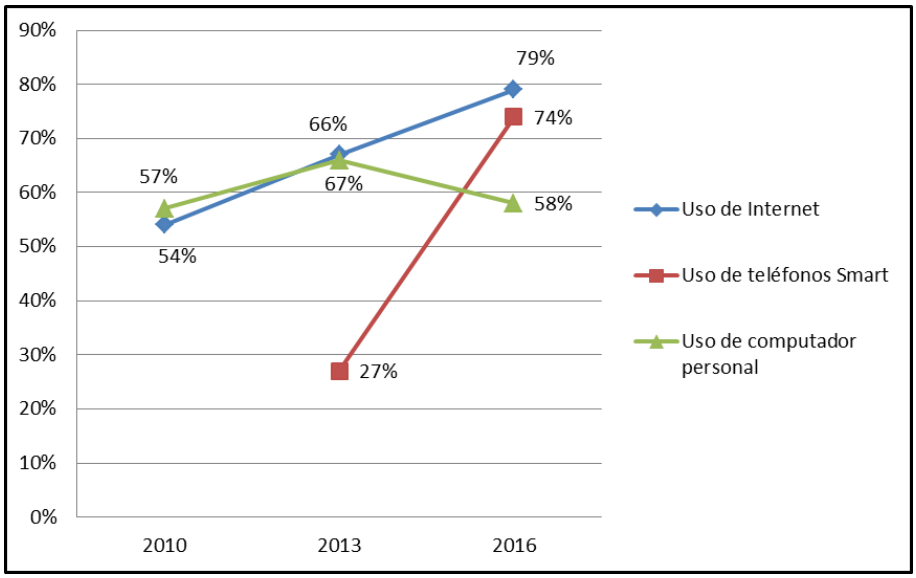
2.1. Las tecnologías de la información y la comunicación

El nivel de desarrollo e inserción de las tecnologías de la información y la comunicación permiten conocer el objeto referente de las políticas de seguridad cibernética que serían implementadas en cada Estado. En los casos de Uruguay y Ecuador, se analizarán indicadores que permitan conocer cuál es el objeto o los objetos referentes, su dimensión e importancia para cada país. Además, se podrá evidenciar de manera cuantitativa, en qué medida las tecnologías de la información y la comunicación se han insertado en el Estado y su población.

2.1.1. El espacio cibernético de Uruguay

Con relación al uso de las tecnologías de la información y la comunicación en Uruguay, las encuestas que realiza el Instituto Nacional de Estadística determinan un crecimiento importante del uso del internet por parte de la ciudadanía. Es decir que, existen muchas más interacciones de la sociedad en el espacio cibernético y, por lo tanto, un crecimiento de este escenario en el país. Las estadísticas evidencian un crecimiento del 25% desde el 2010 al 2016. Las estadísticas también demuestran un incremento importante del uso de teléfonos Smart por parte de la ciudadanía. El 27% utilizaba un teléfono Smart en el 2013, para el 2016 los utilizaban el 74% de la población. Es interesante mencionar que el uso de la computadora personal tuvo un comportamiento diferente. Entre el 2010 y el 2013 se incrementó la población que utilizaba esta herramienta tecnológica del 57% al 66%; sin embargo, el porcentaje se reduce al 58% en el 2016 (AGESIC 2016).

Gráfico 2: Uso del espacio cibernético en Uruguay



Fuente: Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento

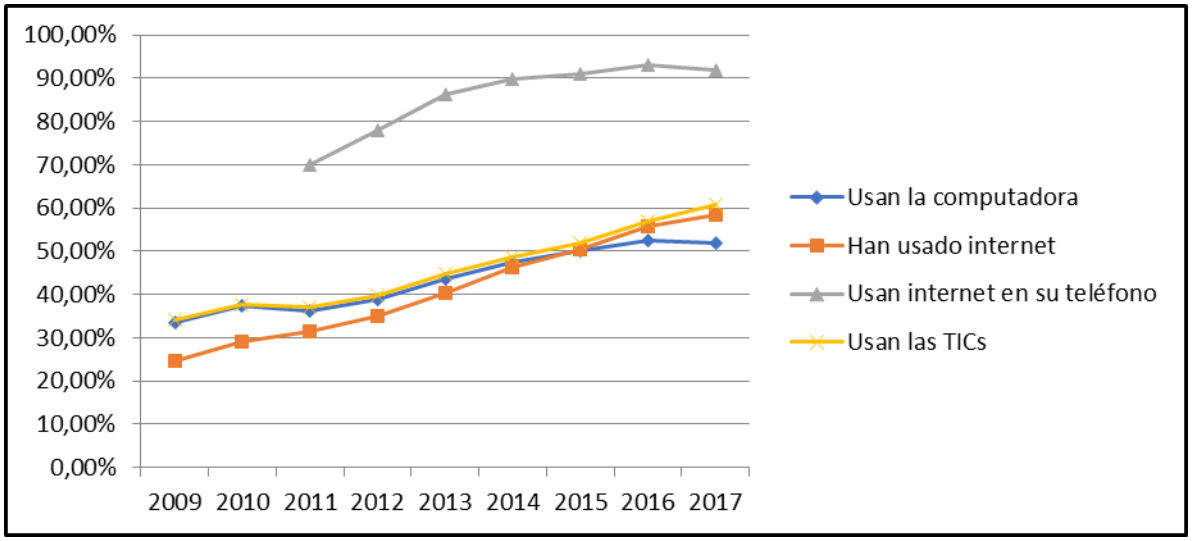
El objeto referente de políticas de seguridad cibernética de Uruguay también puede ser dimensionado a través del desarrollo de gobierno electrónico y la infraestructura de telecomunicaciones. En los informes elaborados por la División de Instituciones Públicas y Gobierno Digital de la Organización de las Naciones Unidas, Uruguay se ubicó en el 2010 en el tercer lugar de los países de la región con el mayor desarrollo de gobierno electrónico y en la misma posición en servicios en línea. En el mismo año, ocupó el primer lugar con mayor infraestructura de telecomunicaciones (UN 2010). Para el 2016, Uruguay se convirtió en el país con el mejor desarrollo de gobierno electrónico de América del Sur, compartió el primer lugar con Chile en términos de servicios en línea y mantuvo el primer lugar en infraestructura de telecomunicaciones (UN 2016).

2.1.2. El espacio cibernético de Ecuador

El Instituto Naciones de Estadísticas y Censos (INEC), junto con el Ministerio de Telecomunicaciones han generado indicadores sobre el acceso y uso de las TICs en el Ecuador. Estas estadísticas dan cuentas de las características del espacio cibernético en el país y del objeto referente al que se refiere el discurso securitizador. En primer lugar, es necesario resaltar el incremento del uso de las TICs a nivel nacional, de un 34% en el 2009 al 61% al 2017. Este incremento porcentual concuerda con el crecimiento en el uso de la computadora y del internet. Además, es importante señalar el alto porcentaje de la población que usa el

internet en su teléfono, 92% para el 2017. Además, de la población ecuatoriana el 8,42% tenía un teléfono Smart en el 2011 y 63,61% en el 2017 (MINTEL 2018).

Gráfico 3: Uso del espacio cibernético en Ecuador



Fuente: INEC, MINTEL

Las encuestas realizadas en Ecuador también permiten conocer datos estadísticos del uso de las tecnologías de la información y comunicación en el sector empresarial. En el 2012, el 95,8% de las empresas ecuatorianas contaban con acceso a internet y el 43,3% con una página web. En el 2015, el 96,6% de las empresas tenían acceso a internet, mientras que el 61,4% tenía una página web. De igual manera, la dimensión del espacio cibernético y del objeto referente puede ser visualizada en el aumento de empresas dedicadas a las TICs. En el año 2012 funcionaban 12177 empresas, las cuales pasaron a ser 14096 para el 2016. La gran mayoría dedicada a la venta de equipos y sistemas de telecomunicación (MINTEL 2018).

El ranking mundial que ha elaborado la División de Instituciones Públicas y Gobierno Digital de las Naciones Unidas, que permitiría dimensionar el espacio cibernético en Ecuador, ha determinado que en el 2010 el país ocupaba la octava posición, de los 10 países de América del Sur, en desarrollo del gobierno electrónico. En servicios en línea, ocupaba la séptima posición y en términos de infraestructura de telecomunicaciones también ocupaba la octava posición en la región (UN 2010). En los datos publicados en el 2016, el espacio cibernético de Ecuador había crecido. En desarrollo de gobierno electrónico y en servicios en línea, ocupaba el sexto lugar; mientras que en infraestructura crítica ocupaba la séptima posición (UN 2016).

Las estadísticas demuestran la dimensión del objeto referente de Ecuador y su crecimiento, en comparación con los otros países de América del Sur.

2.2. La sociedad como audiencia

2.2.1. La sociedad uruguaya

Como resultado de décadas de política pública enfocada en la instauración y fortalecimiento del país en el ámbito tecnológico, Uruguay ha construido una sociedad con conciencia sobre el uso de las TIC, especialmente sobre el uso del internet. Para el año 2015, ya estaba establecida una mentalidad de seguridad cibernética en la población. Solamente Colombia lograba, en ese entonces, el mismo nivel de madurez social[5] en términos de ciberseguridad en la región. En Uruguay, un importante grupo de la ciudadanía tiene el conocimiento y capacidad para asegurar el espacio cibernético en el que interactúa; puede proteger su privacidad y evitar la intromisión no deseada por parte de otros usuarios de la red (BID y OEA 2016).

Según datos proporcionados por los estudios de "Conocimientos, Actitudes y Prácticas de Ciudadanía Digital", en el 2013, el 70% de la población había escuchado sobre delitos de carácter cibernético, el 90% contaba con antivirus en sus computadoras y el 40% había cambiado sus contraseñas de acceso a correos electrónicos o redes sociales (Bertón, Totorica y González 2013). La población uruguaya, además, es cada vez más consciente de la necesidad de seguridad cibernética. Para el año 2017, el 52% de la población realizó cambios en sus redes sociales y el 33% evitó determinados sitios de internet. Por último, es importante mencionar que desde el 2014 al 2017, se han reducido los usuarios de internet que se sienten inseguros y han aumentado aquellos que sienten confianza para realizar, incluso, transacciones en línea (AGESIC 2017).

La sociedad uruguaya se ha involucrado en el proceso securitizador y ha aceptado las políticas de ciberseguridad impulsadas desde el gobierno. Iniciativas como "Seguro te conectás", se han enfocado en concientizar a la población sobre los riesgos y las amenazas del uso de

[5] Durante la presente investigación se hará referencia a la madurez social en consideración con el concepto establecido por la OEA y el BID en su informe "Ciberseguridad ¿Estamos preparados en América Latina y el Caribe?". En dicho informe se menciona que la madurez "define el grado de eficacia con el que una organización ejecuta una competencia en particular dentro de la misión y las autoridades de la organización. La metodología implementada en el informe establece cinco niveles de madurez: inicial, formativo, establecido, estratégico y dinámico; y califica a la madurez social en base a: mentalidad y conciencia de ciberseguridad, confianza en el uso de internet y privacidad en línea.

internet, especialmente en actividades de carácter financiero. Esta campaña nacional inició en 2013 y, para el 2017, alcanzó la participación de más 10 mil personas en las redes sociales que la promocionan. Otra de las iniciativas que han permitido que la audiencia acepte el discurso securitizador es la campaña "Tus datos valen. Cuidalos". Esta propuesta gubernamental ha involucrado a niños, padres y maestros en la protección de información personal que se encuentra en el espacio cibernético. En el 2016, como parte de esta campaña se realizó el concurso "Tus datos cuentan", en el que participaron 1860 niños de todo Uruguay (URCDP 2016).

Esta última campaña es parte de las políticas educativas en ciberseguridad que son implementadas en Uruguay desde el nivel básico de educación hasta los cursos especializados impartidos por el Centro de Altos Estudios Nacionales para cualquier persona interesada en la temática. El acercamiento educativo ha generado un espacio propicio para que la sociedad se identifique con las políticas de seguridad. Además, se promueve un espacio para que grupos específicos de la sociedad, como la academia, también se involucren en el ámbito de la seguridad cibernética, no solo como audiencia, sino que también, como actores securitizadores.

2.2.2. La sociedad ecuatoriana

En el ecuador, la sociedad no ha desarrollado una conciencia de seguridad cibernética. Si bien el Gobierno ha impulsado campañas de seguridad, la población no conoce sobre los ataques cibernéticos, sus repercusiones y las respuestas más apropiadas. "Los ataques cibernéticos se incrementaron significativamente en los últimos años, pero la mayoría de los afectados no conocían los medios más eficaces para la denuncia de estos incidentes" (BID y OEA 2016, 70). Incluso, se considera que la sociedad que conoce sobre los riesgos del espacio cibernético no implementa de manera personal medidas de seguridad. En el ámbito empresarial, la mentalidad de seguridad cibernética se encuentra más desarrollada. El sector privado ha identificado prácticas que estarían en detrimento de su seguridad cibernética. Sin embargo, la conciencia social sobre los riesgos de un ataque cibernético ha ganado espacios en las discusiones sobre el bienestar en materia cibernética en el país (BID y OEA 2016).

Durante el período de estudio, el Ecuador ha impulsado un número reducido de proyectos que buscan concientizar a la población sobre seguridad cibernética. La sociedad, en general, ha podido participar en campañas como "Promoción de una cultura de Inteligencia", que

buscaban concientizar sobre los riesgos y las amenazas cibernéticas (BID y OEA 2016). Además, el gobierno ecuatoriano ha emitido boletines ciudadanos enfocados en la seguridad cibernética a través de la Policía Nacional y a organizado eventos como el "Congreso de Ciberseguridad en Banca y Gobierno" (MINTEL/CDV 2016) o "Ciberseguridad desde la Mitad del Mundo" (ARCOTEL 2016). Ahora bien, incluso cuando estos programas han sido direccionados a la sociedad y enfocados en temas de seguridad cibernética, la sociedad ecuatoriana no ha consolidado una conciencia frente a los ataques informáticos y a la seguridad al momento de utilizar las TICs. La respuesta de la sociedad frente a la securitización de un aspecto, como el espacio cibernético, está alineada a la naturaleza del actor securitizador y su discurso.

2.3. Actores securitizadores y su discurso

La securitización de una temática da inicio con el acto discursivo de un actor securitizador que busca construir un conjunto de mecanismos extraordinarios de política pública para la protección y garantía de un objeto referente. Debido a la organización de los Estados de América del Sur, el actor securitizador de mayor relevancia es el gobierno, principalmente el Presidente como su máximo representante. Sin embargo, otros actores gubernamentales han generado discursos securitizadores que han calado en la audiencia. Cada actor es diferente en determinado caso. La participación en el discurso securitizador depende, de entre una gran variedad de factores, de la estructura del gobierno y de la capacidad de influencia de los representantes gubernamentales de las instituciones que la conforman.

2.3.1. Gobierno electrónico y seguridad uruguaya

En el caso uruguayo, el principal actor securitizador es el gobierno nacional y su mayor representante, el presidente de la república. El discurso de los actores securitizadores se fue introduciendo de manera paulatina en documentos de política pública, decretos y leyes, que buscaban, principalmente, el desarrollo e implementación de las TIC en las instituciones públicas. La consolidación de un gobierno electrónico[6] en Uruguay motivó a la administración pública a considerar los aspectos de seguridad en este ámbito. En este apartado se analizará el rol del gobierno en el proceso securitizador del espacio cibernético, su discurso y prácticas; así como la influencia de otros actores que participaron en el proceso.

[6] El Banco Mundial define al gobierno electrónico como el "uso de tecnologías de información por parte de las agencias gubernamentales que tienen la habilidad de transformar las relaciones entre los ciudadanos, los negocios y otros brazos del gobierno" (Pereiro Alonso 2011)

2.3.1.1. Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento

Una institución gubernamental que resulta indispensable para la securitización del espacio cibernético es la Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento (AGESIC). Esta organización, fue creada en el 2005 por medio del decreto No.17930. Sin embargo, fue fundada el 24 de septiembre de 2007. Desde su creación ha sido una unidad indispensable para la consolidación de una sociedad de la información, el desarrollo tecnológico de las instituciones del Estado y la ejecución de políticas direccionadas al ámbito informático[7].

Uno de los objetivos estratégicos de esta agencia es "dictar y proponer políticas, normas y estándares informáticos en el Estado y fiscalizar el cumplimiento de la normativa vigente en materia informática" (AGESIC 2014). Esta competencia le otorga la capacidad de moldear e impulsar un discurso securitizador para el espacio cibernético. Además, entre sus cometidos, la AGESIC tiene como responsabilidad "generar, planificar y ejecutar proyectos de Gobierno Electrónico con énfasis en la mejora de los servicios a todas las personas" (AGESIC 2014). En el cumplimiento de sus objetivos y competencias, desde el 2007, en representación del gobierno uruguayo, la AGESIC ha emitido cuatro agendas para el ámbito digital del país. El análisis de estas agendas permite observar cómo van calando medidas de seguridad en la política pública a ser implementada.

2.3.1.2. Agendas digitales de Uruguay

La estrategia para el establecimiento del espacio cibernético y para el uso de las TIC en Uruguay está centrada en cuatro pilares fundamentales: la consolidación de un gobierno digital, la construcción de una sociedad basada en la información y el conocimiento, el uso de tecnologías para un gobierno abierto y transparente y la innovación. Cada uno de estos pilares enmarcan el contexto del proceso securitizador y funcionan como espacios para la difusión del discurso del principal actor securitizador. Sin embargo, las agendas digitales son las herramientas principales por las cuales incursionan los mecanismos extraordinarios que permiten garantizar la seguridad de todos los elementos del Estado, mientras que, los otros tres pilares desarrollan el escenario en el cual se aplicarán dichas medidas.

[7] Ley No 17930. Presupuesto nacional de sueldos gastos e inversiones. Ejercicio 2005 – 2009. Publicada D.O. 23/12/2005

La primera agenda digital de Uruguay, establecida en 2007, se enfocó en la institucionalización e implementación de instrumentos tecnológicos y, por lo tanto, no consideró como prioritaria la seguridad cibernética. Los siete objetivos[8] establecidos en este plan se enfocaron en el desarrollo e inserción de la tecnología en la sociedad uruguaya en los aspectos educativos, productivos, sociedad civil, sectores desfavorecidos y administración pública. Además, se consideró prioritaria la consolidación de cooperación e integración regional para el intercambio de información (AGESIC 2007).

Si bien este plan no cuenta con objetivos específicos de seguridad, da inicio al proceso securitizador al mencionar como parte de sus metas para la promoción del gobierno electrónico a los servicios de seguridad. Asimismo, esta agenda promovió la consolidación del marco normativo para la digitalización del país. En esta área, se impulsó una ley para la protección de los datos de la ciudadanía. Esta ley representa una medida de carácter extraordinario con el fin de garantizar un derecho inherente al ser humano (AGESIC 2007). La inclusión de metas de esta naturaleza marca el inicio del proceso securitizador del espacio cibernético en Uruguay.

La segunda agenda digital, promulgada en el 2008, abordó de manera más específica la seguridad en el espacio cibernético. Este plan tomó como referencia los objetivos de la agenda digital de 2007 y los consideró como líneas estratégicas que direccionaron los objetivos y metas del gobierno hasta el 2010. Los 22 objetivos de esta agenda buscaron la consolidación de la sociedad informática en Uruguay en los mismos espacios, por lo tanto, se los considera como la segunda fase de institucionalización e implementación de las TICs. No obstante, establece la consolidación de proyectos específicos de seguridad cibernética (AGESIC 2008).

Al igual que la agenda precedente, determina como metas la implementación del gobierno electrónico y la oferta de servicios de seguridad. Pero, además, se establecen como metas la creación de unidades operativas encargadas de la protección de datos, el acceso a la información y a la respuesta de incidentes. El carácter performativo del discurso securitizador plasmado en este plan, permitió la creación del Centro de Repuesta a Incidentes Informáticos

[8] Objetivos de la Agenda Digital Uruguay 2007 – 2008: Objetivo 1 “equidad e inclusión social”, objetivo 2 “fortalecimiento democrático”, objetivo 3 “transformación del Estado”, objetivo 4 “desarrollo de infraestructura”, objetivo 5 “desarrollo productivo de la industria”, objetivo 6 “educación y generación de conocimiento, y, objetivo 7 “integración e inserción regional” (AGESIC 2007)

de Uruguay. Una unidad que funciona como uno de los principales instrumentos de seguridad cibernética del país y en el cual profundizaremos posteriormente (AGESIC 2008). A partir de este plan, se puede visualizar el desarrollo del proceso securitizador por medio de la ampliación del discurso y su materialización a través de la creación de instrumentos específicos de seguridad cibernética.

La tercera agenda digital de Uruguay profundiza el discurso securitizador, pero, en comparación con la agenda previa, no aborda la ciberseguridad de manera explícita ni la establece como uno de los objetivos o metas del gobierno entre el 2011 y 2015. Esta agenda se enfocó en la expansión del gobierno electrónico y de la sociedad de la información. Se mantienen las mismas líneas estratégicas establecidas desde la primera agenda digital; sin embargo, los objetivos buscan universalidad de los recursos tecnológicos e informáticos y su uso por parte de toda la sociedad uruguaya. Para esta agenda "las TIC pueden y deben constituirse en una herramienta para continuar mejorando el bienestar de la ciudadanía y el desarrollo nacional" (AGESIC 2011, 3).

La aplicación del espacio cibernético por medio del uso de las TIC hizo "crítico establecer un marco habilitante para su buen uso" (AGESIC 2011, 3). La tercera agenda se enfocó en los mecanismos de seguridad para la provisión de redes avanzadas en el ámbito de la salud. La promulgación de medidas extraordinarias de carácter securitista para la protección de un objeto referente como el ámbito de la salud, permite que la audiencia acepte el discurso securitizador con mayor facilidad. Además, la participación de actores específicos y de la ciudadanía uruguaya en la construcción de esta agenda creó condiciones facilitadoras para el proceso securitizador del espacio cibernético (AGESIC 2011).

El último plan emitido por el gobierno uruguayo, la agenda digital hasta al año 2020, busca la transformación del espacio cibernético, la profundización del gobierno electrónico y la consolidación de la sociedad de la información. A diferencia de las agendas previas que se organizan alrededor de siete líneas estratégicas. La agenda "está estructurada a partir de cuatro pilares, que nuclean una serie de objetivos y compromisos concretos con metas específicas y constatables" (AGESIC 2016, 8). Estos pilares son: "políticas sociales e inclusión, desarrollo económico sustentable, gestión de gobierno y gobernanza para la sociedad de la información" (AGESIC 2016, 9). Todos ellos enfocados en el desarrollo de la gestión cibernética en el país.

Este plan, a diferencia de las agendas previas, demuestra el proceso securitizador y la característica performativa del discurso, impulsada por la intersubjetividad de los actores relacionados a la sociedad de la información en Uruguay. Es por este motivo, que esta agenda incorpora objetivos específicos de ciberseguridad. "En el Uruguay digital convergen esfuerzos de diversos actores de los sectores público y privado, la academia, la sociedad civil organizada y la comunidad técnica" (AGESIC 2016, 7). La participación de varios actores de la sociedad uruguaya facilita la aceptación del discurso y de medidas extraordinarias por parte de la audiencia. Incluso, este plan promueve la creación de mecanismos e instrumentos específicos para garantizar la seguridad en el uso de las TIC.

Específicamente, el octavo objetivo de la agenda digital de Uruguay al 2020 busca generar entornos de confianza en el uso de la tecnología. Es decir que, el objetivo propone la construcción de "entornos seguros y formas de interacción basadas en la confianza, que promuevan la plena participación en la sociedad de la información" (AGESIC 2016, 18). Las metas alineadas a este objetivo proponen la creación y actualización de marcos normativos adecuados para la protección del internet, del usuario y para la repuesta a las amenazas cibernéticas. Además, propone la profundización del acto discursivo para la sensibilización de la sociedad uruguaya frente a la necesidad de establecer mecanismos específicos de seguridad cibernética. Por último, la agenda plantea la creación de un Centro Nacional de Operación de Ciberseguridad, encargado específicamente de este ámbito (AGESIC 2016).

2.3.1.3. Los otros tres pilares del Uruguay digital

La consolidación de una sociedad de la información y el conocimiento en Uruguay no solo establece un escenario favorable para que el discurso securitizador se materialice en prácticas e instrumentos. Además, una sociedad cada vez más relacionada a las TIC considera necesarias medidas específicas para la protección, en el espacio cibernético, de diversos objetos referentes, principalmente la información. El gobierno uruguayo busca el establecimiento de una sociedad con "actividades de creación, distribución y manipulación de la información y el conocimiento" (AGESIC 2011, 2). Así como la paulatina disminución de la brecha digital a través de la difusión del uso de las TIC.

Los alcances de la agenda hacia una sociedad de la información en Uruguay se demostraron en una encuesta de uso de las TIC. Para el 2016, el 70% de la sociedad uruguaya tenía una computadora y el 83% tenía acceso a internet en sus hogares (AGESIC & INE 2016). La alta

relación de la ciudadanía con la tecnología y su amplia interacción en el espacio cibernético establece un escenario favorable para establecer una intersubjetividad de la necesidad de seguridad cibernética, en el que la gran mayoría de la audiencia del discurso securitizador participa activamente en el espacio cibernético y hace uso de herramientas tecnológicas.

El gobierno de Uruguay ha elaborado tres planes para la consolidación de un Gobierno Abierto en el que se promulgan principios de transparencia y participación social por medio de herramientas electrónicas. Estos planes impulsados desde el 2012[9], en el gobierno del presidente José Mujica utilizan los mecanismos del gobierno electrónico "como una oportunidad de transformación del Estado desde una visión innovadora, haciendo uso intensivo de la tecnología y teniendo como fin construir un Estado enfocado en el ciudadano" (Presidencia de la República Oriental del Uruguay 2012, 2). Estos planes complementan el proceso de securitización del espacio cibernético al impulsar medidas de responsabilidad y protección de derechos ciudadanos en el uso de estas tecnologías.

El último pilar de la estrategia Uruguay digital se basa en la innovación a partir de la generación de análisis estratégicos, elaboración de estudios y escenarios prospectivos. La innovación de la agenda informática enmarca el trabajo de una red de observatorios: "Observatorio de la Sociedad de la Información y el Conocimiento, Observatorio de la Ciudadanía Digital, Observatorio Jurídico y Observatorio Tecnológico" (AGESIC 2014). Los productos resultantes del trabajo de la red de observatorios aportan al desarrollo y perfeccionamiento de las agendas para el uso de las TIC en el país. Además, la red aporta al discurso securitizador al incorporar argumentos académicos y premisas específicas para la securitización del espacio cibernético.

2.3.2. Gobierno electrónico y seguridad ecuatoriana

El Ecuador no cuenta con una estrategia específica de ciberseguridad. Si bien el gobierno ha trabajado por el desarrollo de mecanismos que permitan hacer frente a las amenazas de carácter informático, no se ha logrado consolidar políticas de seguridad que se enfoquen en esta materia. A pesar de estas limitaciones, existen varios actores securitizadores que han buscado impulsar, en sus ámbitos respectivos, ciertos proyectos de seguridad cibernética. Los principales actores gubernamentales están estrechamente relacionados con las tecnologías de

[9] Plan de Acción Uruguay 2012-2014, 2do Plan de Acción Uruguay 2014-2016 y 3er Plan De Acción Nacional de Gobierno Abierto de Uruguay 2016-2018

la información y la comunicación. En el presente apartado se detallará como los actores securitizadores ecuatorianos han influenciado en el limitado proceso de construcción de políticas de seguridad cibernética.

2.3.2.1. Ministerio de Telecomunicaciones y de la Sociedad de la Información

La institución pública encargada de las tecnologías de la información y comunicación en el Ecuador es el Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL). Este ministerio busca "coordinar la política del sector de las telecomunicaciones, orientada a satisfacer las necesidades de toda la población" (MINTEL 2018). Sus políticas se encuentran enfocadas en el desarrollo del país y el acercamiento del Estado con los ciudadanos, a través del uso de las TIC; así como, la consolidación de las tecnologías de la información y comunicación como los ejes de "transformación productiva y desarrollo económico" (MINTEL 2018).

El MINTEL fue creado en 2009, mediante decreto ejecutivo del expresidente Rafael Correa. En el decreto de creación de este importante ministerio se atribuye la competencia para "[…] formular las políticas y planes para la creación, regulación y supervisión de la Central de Datos del Ecuador, intercambio de información por medios electrónicos, seguridad en materia de información e informática, así como la evaluación de su ejecución […]"[10]. La Ley Orgánica de Telecomunicaciones, en su Artículo 140, establece que esta institución es la encargada "de la telecomunicación y de la sociedad de la información y las comunicaciones y de la seguridad de la información"[11]. Es importante mencionar que, en esta ley, se promueve el discurso del uso del espectro radioeléctrico para la seguridad pública y del Estado.

En el marco de sus competencias, el MINTEL promovió, en el 2016, la expedición del "Plan Nacional de Telecomunicaciones y Tecnologías de Información". En este Plan se han establecido cuatro macro objetivos enfocados en el impulso de las herramientas tecnológicas e informáticas como mecanismos para el desarrollo de aspectos sociales y económicos del Ecuador (MINTEL 2016). Si bien esta institución pública ha sido responsable del fomento de políticas relacionadas al espacio cibernético, otra institución que tuvo una importante

[10] Decreto Ejecutivo No. 8. Créase el Ministerio de Telecomunicaciones y de la Sociedad de la Información como órgano rector del desarrollo de las tecnologías de la información y comunicación. Registro oficial No. 10. 24 de agosto de 2009.
[11] Ley Orgánica de Telecomunicaciones. Registro oficial Suplemento 439. 18 de febrero de 2015.

relevancia para el impulso del discurso securitizador fue la Secretaría Nacional de la Administración Pública.

2.3.2.2. Secretaría Nacional de la Administración Pública

En el 2002, el Ecuador creó la Secretaría Nacional de la Administración Pública (SNAP) con el fin de asesorar y asistir a la Presidencia del Ecuador en todos los aspectos relacionados a la adopción y ejecución de política pública[12]. En el 2013, la SNAP absorbe a la Secretaría Nacional de Transparencia de Gestión y, por lo tanto, se encargó del complimiento de sus competencias[13]. Durante el funcionamiento de esta institución pública, antes de su disolución en 2017, se impulsaron políticas de consolidación del uso de las TICs y proyectos específicos de seguridad cibernética en la administración pública.

Por medio de la SNAP, se creó la Comisión para la Seguridad Informática y de las Tecnologías de la Información y Comunicación. En el Acuerdo Ministerial de esta Comisión se menciona que "los instrumentos tecnológicos de información y comunicación son herramientas imprescindibles para el cumplimiento de la gestión institucional e interinstitucional […] y en tal virtud deben cumplir con estándares de seguridad acorde a la dinamia en que se desarrolla la Administración Pública"[14]. Esta Comisión estaba conformada por la SNAP, la Presidencia de la República y la Secretaría Nacional de Inteligencia. En un acuerdo posterior se integró el MINTEL a la Comisión. Las cinco funciones de la Comisión estaban enfocadas en: el análisis del estado de las herramientas informáticas, los lineamientos de seguridad cibernética, la formulación de planes de normas y protocolos, así como, la presentación de recomendaciones sobre el manejo de las TICs en las entidades públicas[15].

Uno de los esfuerzos más importantes de la SNAP, junto con la Comisión para la Seguridad Informática y de las Tecnologías de la Información y Comunicación, por impulsar la seguridad cibernética en Ecuador, fue el "Esquema Gubernamental de Seguridad de la Información". Mediante el Acuerdo ministerial 166 "se establece las directrices y

[12] Decreto Ejecutivo No. 2428. Expídase el Estatuto del Régimen Jurídico y Administrativo de la Función Ejecutiva. Registro oficial No. 536. 18 de marzo de 2002.
[13] Decreto Ejecutivo No. 1522. Créase la Secretaría Nacional de Gestión de la Política. Registro oficial No. 13. 12 de junio de 2013.
[14] Acuerdo Ministerial 804. Créase la Comisión para la Seguridad Informática y de las Tecnología de la Información y Comunicación. Registro oficial 511. 11 de agosto de 2011.
[15] Acuerdo Ministerial 804. Créase la Comisión para la Seguridad Informática y de las Tecnología de la Información y Comunicación. Registro oficial 511. 11 de agosto de 2011.

lineamientos para la Seguridad de la Información dentro de las entidades de la Administración Pública Central Institucional y dependiente de la Función Ejecutiva" (Secretaría Nacional de la Administración Pública 2014, 31).

Este acuerdo considera que "la Administración Pública de forma integral y coordinada debe propender a minimizar o anular riesgos en la información, así como proteger la infraestructura gubernamental, más aún si es estratégica, de los denominados ataques informáticos o cibernéticos"[16]. La estrategia determina para las instituciones públicas su política de seguridad de la información, la organización de la seguridad, la adquisición y manejo de activos y la respuesta frente a incidentes de cibernéticos. Este acuerdo puede ser considerado como uno de los elementos discursivos más claros en temas de seguridad cibernética del Gobierno ecuatoriano, por su especificidad en los ámbitos que aborda.

2.3.2.3. Plan Nacional de Gobierno Electrónico

El Gobierno del Ecuador mediante la Secretaría Nacional de la Administración Pública (SNAP), institución que fue disuelta el 24 de mayo de 2017, promovió el Plan Nacional de Gobierno Electrónico[17] 2014 – 2017. Este Plan se alineó con los objetivos establecidos en los planes de desarrollo del Ecuador. Este documento buscó "consolidar un Estado cercano, abierto, eficiente y eficaz, para lo cual establece un modelo para el desarrollo de Gobierno Electrónico" (Secretaría Nacional de la Administración Pública 2014). Los tres objetivos estratégicos planteados en el Plan son: gobierno cercano, gobierno abierto y gobierno eficiente y eficaz. Para lograr el cumplimiento de estos objetivos, la SNAP consideró fundamental trabajar en el marco regulatorio, los servicios y procesos, tecnologías de la información y comunicaciones; y, personas (Secretaría Nacional de la Administración Pública 2014, 9).

El gobierno ecuatoriano consideró doce principios relacionados al desarrollo de un gobierno electrónico en su Plan 2014 – 2017. Entre estos principios tres principios están directamente relacionados con la seguridad de las tecnologías de la información y la comunicación. El

[16] Acuerdo Ministerial 166. Esquema Gubernamental de Seguridad de la Información. Registro oficial No. 88. 25 de septiembre de 2013.

[17] "Según la Organización de las Naciones Unidas, se refiere al uso de las Tecnologías de Información y Comunicación (TIC) por parte de las instituciones de gobierno para: mejorar cualitativamente los servicios e información que se ofrecen a las ciudadanas y ciudadanos, aumentar la eficiencia y eficacia de las gestión pública, así como para incrementar sustantivamente la transparencia del sector público y la participación ciudadana" (Secretaría Nacional de la Administración Pública 2014, 10).

principio de proporcionalidad “garantiza que los requerimientos de seguridad sean adecuados a la naturaleza de la relación que se establezca con la administración” (Secretaría Nacional de la Administración Pública 2014, 11). Este principio busca diferenciar los niveles de ciberseguridad necesarios para cada administración. Por lo tanto, la seguridad que se implementa en una institución o en otra, variaría dependiendo de su competencia y del tipo de información que manejan.

El segundo principio es el de adecuación tecnológica “recomienda el uso de estándares abiertos y de software libre debido a la seguridad” (Secretaría Nacional de la Administración Pública 2014, 11). Este principio también busca diferenciar a las diferentes instituciones del Estado, e incluso, diferencia a los diferentes administradores de las tecnologías de la información y comunicación en una misma institución. El tercer principio, el que está directamente relacionado al tema de estudio de la presente tesis, es el principio de seguridad y confianza. Éste “garantiza la protección y resguardo de la información y datos, manteniendo sus disponibilidad, confidencialidad e integridad” (Secretaría Nacional de la Administración Pública 2014, 11). Es decir que, este último principio incorpora al discurso securitizador del Plan.

De igual manera, ejerciendo el rol de discurso securitizador, el Plan plantea cuatro pilares para alcanzar los objetivos de Gobierno Electrónico establecidos. Entre los cuatro pilares, los que han planteado acciones direccionadas al ámbito de seguridad son: el marco regulatorio y las tecnologías de la información y comunicaciones. El segundo pilar se refiere específicamente a las capacidades materiales, tecnológicas, que permitan impulsar acciones relacionadas a la seguridad cibernética. Por un lado, el plan busca impulsar la creación de una plataforma de autentificación que permita a los usuarios acceder a una identidad en el espacio cibernético de manera segura. Por otro lado, este pilar promueve el establecimiento de un anillo institucional que abarque niveles específicos de seguridad durante la interacción de los usuarios en el ciberespacio (Secretaría Nacional de la Administración Pública 2014).

2.4. Ecuador y Uruguay: semejanzas y diferencias de los factores lingüísticos del discurso securitizador

Una vez descritas las características de los factores internos del discurso securitizador del espacio cibernético en cada uno de los países de análisis, Ecuador y Uruguay, se pueden comparar los factores internos que pondrían en evidencia la disparidad en la consolidación de

agendas de seguridad cibernética a nivel nacional. En este apartado, se abordarán las diferencias y semejanzas del objeto referente, de la audiencia y del actor securitizador.

Con relación al primer factor, el objeto referente, en este caso el espacio cibernético de Ecuador y Uruguay, han mantenido un constante crecimiento en proporcionalidad con el desarrollo de las tecnologías de la información y la comunicación, impulsado por el Estado y demás actores de la población. En el período de análisis, se puede observar un crecimiento considerable del uso del internet y del alto porcentaje de la ciudadanía que utiliza teléfonos Smart. Además, los gobiernos de los dos países han fomentado el uso de las TICs para facilitar el servicio de las instituciones del Estado, impulsando el crecimiento del espacio cibernético a la administración pública. El espacio cibernético es también un escenario para la interacción comercial y, por lo tanto, las empresas han accedido en su gran mayoría a sistemas informáticos y tecnológicos.

Si bien los dos países han mantenido un considerable desarrollo del espacio cibernético, Uruguay presenta mayor crecimiento en comparación con Ecuador. Como se manifestó previamente, Uruguay ocupa los primeros lugares entre los países de la región, mientras Ecuador ocupa los últimos lugares, en desarrollo de gobierno electrónico, servicios en línea e infraestructura de telecomunicaciones. Es decir que, con relación al objeto referente, la dimensión del espacio cibernético de Uruguay es más amplia en comparación al espacio cibernético de Ecuador.

Tabla 1: Posiciones en el ranking mundial de la División de Instituciones Públicas y Gobierno Digital de las Naciones Unidas

	2010		**2016**	
	Ecuador	**Uruguay**	**Ecuador**	**Uruguay**
Desarrollo del gobierno electrónico	8vo	3ro	6to	1ro
Servicios en línea	7mo	3ro	6to	1ro
Infraestructura de telecomunicaciones	8vo	1ro	7mo	1ro

Fuente: División de Instituciones Públicas y Gobierno Digital de las Naciones Unidas

Como se ha detallado en este capítulo, tanto los gobiernos de Ecuador y Uruguay han impulsado la consolidación de gobiernos electrónicos y sociedades de la información. En los dos casos de estudio el desarrollo de la tecnología y la difusión del uso de la red impulsarían

el desarrollo del país. Sin embargo, el establecimiento del objeto referente en Uruguay, alineado a los planes de desarrollo tecnológico, han difundido el uso de equipos tecnológicos y la interacción del espacio cibernético en la ciudadanía en general. En Ecuador, los esfuerzos estatales se enfocaron en el desarrollo de servicios institucionales públicos basados en las TICs. Por lo tanto, en Ecuador el objeto referente se ubicó principalmente en las instituciones de gobierno y no en la ciudadanía en general.

El desarrollo del objeto referente y quién interactúa con él es importante debido a que los procesos de securitización y el establecimiento de agendas de seguridad cibernética, al ser construcciones basadas en la intersubjetividad, dependen en gran medida del rol de la audiencia. En el caso de los países analizados, el desarrollo del espacio cibernético se ha relacionado con una inclusión de la sociedad en el uso de las tecnologías de la información y comunicación y, en ciertos casos, la creación de una conciencia de seguridad que permite a la ciudadanía aceptar el discurso securitizador del ciberespacio. Tanto en Ecuador, como en Uruguay, la seguridad cibernética se ha insertado en la conciencia ciudadana; sin embargo, la diferencia de este factor entre los dos países es significativa.

La madurez de la sociedad en el uso de las tecnologías de la información y comunicación es mayor en Uruguay. Es por este motivo que la mayoría de la población tiene consciencia de los riesgos y amenazas a las que se enfrenta al interactuar en el espacio cibernético. Un importante número de ciudadanos están en la capacidad de auto asegurarse al momento de utilizar redes de comunicación o el internet. Principalmente, se han impulsado las capacidades relacionadas a la protección de la privacidad y a la intromisión en redes. La sociedad ecuatoriana, por su lado, no ha logrado este nivel de desarrollo en temas de seguridad cibernética. La población ecuatoriana no conoce los riesgos y vulnerabilidades del espacio cibernético. Pero, incluso cuando los conoce, no implementa medidas personales de seguridad.

En Uruguay, la sociedad participa activamente en eventos relacionados a la difusión del discurso securitizador. Desde las instituciones del gobierno, se ha promovido la concientización en la población uruguaya mediante programas enfocados en personas de diversas edades. Incluso, se han impulsado políticas educativas en ciberseguridad desde el nivel básico hasta el nivel superior. En este último nivel, es indudable el respaldo de la academia en el proceso securitizador del espacio cibernético. Ahora bien, incluso cuando el

Ecuador también ha fomentado la participación ciudadana en el proceso securitizador del espacio cibernético, no ha impulsado programas que incluyan a la mayoría de la población. Y, aún, cuando el rol de la academia también ha influenciado en la seguridad cibernética, la audiencia ecuatoriana no ha sido, en igual medida, participe del discurso securitizador, peor aún, de la construcción de una agenda de seguridad cibernética.

El último factor interno del proceso intersubjetivo del discurso de seguridad en el espacio cibernético es el actor securitizador. En Ecuador y Uruguay los gobiernos de turno son los actores securitizadores de mayor relevancia. La legitimidad y autoridad sobre el manejo del Estado, permite a las instituciones gubernamentales impulsar en mayor medida el discurso securitizador del ciberespacio. En los dos casos, el mayor representante del gobierno es el Presidente; sin embargo, estos actores no han tenido roles relevantes al momento de emitir discursos securitizadores. Los actores securitizadores y los discursos más relevantes, tanto en Ecuador como Uruguay, son emitidos por las instituciones gubernamentales, las cuales generaron planes que han buscado impulsar programas o proyectos enfocados en la seguridad de las TICs y de la información que contiene el ciberespacio. Además, en los dos casos, el ordenamiento normativo es empleado como un medio de difusión del discurso securitizador del espacio cibernético, pero además, la misma normativa se convierte en un instrumento que fortalece la continuación de los procesos de construcción de agendas de ciberseguridad.

Ahora bien, en Uruguay, a diferencia de Ecuador, el actor securitizador de mayor relevancia es la Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento (AGESIC). Todos los esfuerzos securitizadores de Uruguay están centrados en esta institución gubernamental. En Ecuador, por otro lado, el discurso securitizador ha sido impulsado por diversas instituciones como: el Ministerio de Telecomunicaciones, la Agencia de Regulación de las Telecomunicaciones, e incluso instituciones públicas que fueron eliminadas, como la Secretaría Nacional de la Administración Pública. Si bien en Ecuador ha existido más actores securitizadores gubernamentales, la coordinación y fuerza del discurso securitizador de Uruguay son mayores.

Una diferencia importante del actor securitizador, es la temporalidad con la cual se inicia el discurso que fomenta la seguridad del ciberespacio. En Uruguay, se pueden identificar elementos claros de seguridad cibernética a partir del año 2008. La Agenda Digital de Uruguay incorpora metas enfocadas en la oferta de servicios de seguridad y respuesta de

incidentes. Es, a partir de ese año, que el discurso securitizador se fue profundizando y ampliando en el país. En Ecuador, a partir del 2014 dio inicio la difusión de un discurso securitizador enfocado en la seguridad del espacio cibernético. Este discurso en Ecuador ha mantenido, en gran medida, su enfoque en la seguridad de la información en las instituciones públicas.

A partir de lo previamente mencionado se pueden identificar las dos últimas diferencias en el tercer factor interno de análisis. Como se mencionó previamente, el discurso securitizador del espacio cibernético en Ecuador se ha enfocado, primordialmente, en la información manejada por el sector público. Este enfoque está relacionado a la limitada participación de otros actores no gubernamentales que aporten a la securitización en Ecuador. En Uruguay, la participación de otros actores, alejados de la esfera gubernamental, ha sido relevante. Es así como, la sociedad no solo se ha desenvuelto como audiencia, sino además, varios grupos se han transformado en actores securitizadores que impulsan con su discurso la construcción de seguridad cibernética en Uruguay. El sector privado y la academia han sido actores securitizadores del espacio cibernético importantes. Esta diversidad de actores también ha permitido que el discurso securitizador en este país se enfoque en una mayor diversidad de ámbitos de interacción social en el espacio cibernético.

Capítulo 3
Factores externos del discurso de seguridad cibernética

3.1. Historia de la seguridad cibernética y su contexto actual

3.1.1. Uruguay antes de la seguridad informática

Como se mencionó previamente, la comprensión del contexto histórico permite establecer condiciones que aportan al proceso securitizador del espacio cibernético. La historia digital de Uruguay, específicamente del sector público, nace con la creación de una Comisión asesora que tuvo como objetivo "estudiar la utilización y aprovechamiento integral de los equipos eléctricos y electrónicos de procesamiento de datos"[18]. Durante su existencia, entre 1979 y 1991, se integró momentáneamente al Consejo de Seguridad Nacional por medio del Decreto No 515/979. Las limitaciones y falta de cumplimiento de sus objetivos impulsaron su eliminación en el año 2005, junto con la supresión de otras instituciones relacionadas a este ámbito.

Entre las instituciones que desaparecieron en el 2005, se encontraba el Comité Ejecutivo para la Reforma del Estado (CEPRE). Este comité de la denominada Oficina de Planeamiento y Presupuesto fue creado por medio de la Ley No 16736 en 1996. Sus actividades se enfocaban en la modernización del Estado. En el marco de sus competencias, el Comité se vinculó al desarrollo de los sistemas de información de las instituciones públicas. Entre sus aportes, los de mayor relevancia, en el ámbito cibernético, fueron el desarrollo del Sistema Integrado de Compras Estatales y el portal web del gobierno de Uruguay. A pesar de sus grandes contribuciones a la tecnificación del Estado, no logró impulsar una agenda de políticas públicas para el ámbito informático (Pardo, Monteverde y D.Ríos 2008).

Un tercer organismo relevante en el contexto que impulsó un proceso de securitización en Uruguay es el Comité Nacional para la Sociedad de la Información (CNSI). Este organismo fue creado en el 2000 con el objetivo de fomentar el desarrollo de una sociedad de la información. Los miembros que integran este Comité es una de sus peculiaridades más relevantes. Entre sus participantes están: el presidente de la República de Uruguay, como representante político; rectores de universidades públicas y privadas, como representantes de la academia; y, presidentes del área técnica de telecomunicaciones e informática, como

[18] Decreto No 510/969. Comisión asesora. Informática. Publicación D.O. 15/10/1969

expertos en la materia. Esta multiplicidad de actores permitiría, a posteriori, influenciar en varios sectores de la seguridad cibernética.

Desde su formación, el Comité Nacional para la Sociedad de la Información, ha tenido entre sus objetivos "crear las condiciones para definir una política nacional concertada que permita el desarrollo de la sociedad de la Información en el Uruguay"[19]. Este comité impulsó el desarrollo y crecimiento del espacio cibernético, a través de la promoción de las tecnologías de la información y comunicación para su implementación en los ámbitos público y privado. Además, plasmó una de las estrategias a nivel país más importantes para la incursión de nuevas tecnologías en todos los aspectos de la sociedad y el gobierno. Esta estrategia fue denominada Uruguay en Red (Presidencia de la República de Uruguay 2000).

Uruguay en Red es el cuarto pilar contextual de la base sobre la que se construye un proceso de securitización del espacio cibernético en ese país. La estrategia abarca cuatro programas prioritarios: Internet en la Enseñanza, un programa de conectividad educativa; Gobierno en Red, un programa de modernización de toda la administración pública; Proyecto Mercurio, un programa de acceso a Internet; y, Uruguay Tecnológico, un programa para apoyar al desarrollo de software. El trabajo realizado en la "implementación de acciones concretas, formulación de proyectos, negociación ante organismos internacionales [y la] creación de marcos de entendimiento" (Presidencia de la República de Uruguay 2000, 3) generó un desarrollo exponencial del espacio cibernético de Uruguay. Sin embargo, sus objetivos no abarcaron la seguridad y garantía de estos nuevos planes, políticas e instrumentos a ser implementados en el país, y en especial, no se consideró a la seguridad cibernética como un eje de acción.

Así, para el año 2005, el gobierno uruguayo decidió crear la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento. A partir del decreto para su formación, se le asignaron los objetivos de la Comisión Nacional de Informática (CONADI) y del Comité Nacional para la Sociedad de la Información (CNSI);

[19] Decreto No 225/000. Creación del Comité Nacional para la Sociedad de la Información. Publicado D.O. 17/08/2000

además, se le hizo cargo de todos los proyectos tecnológicos del Comité Ejecutivo para la Reforma del Estado (CEPRE)[20].

3.1.2. Ecuador antes de la seguridad informática

Durante el mismo período, Ecuador vivía su propio contexto histórico de desarrollo del espacio cibernético. El país empezó su interacción en la red en 1989 como uno de los pioneros a nivel regional. Sin embargo, al inicio del siglo XXI "Ecuador presenta una densidad de usuarios cinco veces menor que el promedio de todos los países de América" (Rocca 2001, 41). Incluso con las limitaciones a las que se enfrentaba el país, el Gobierno ecuatoriano fomentaba políticas que impulsen el avance de las tecnologías de la información y la comunicación en el territorio. Una de las primeras propuestas consideró al aspecto de seguridad. La Ley para la Transformación Económica del Ecuador del 2000, estipulaba en su Artículo 38 que,

> los servicios de telecomunicaciones se brindarán en régimen de libre competencia, evitando los monopolios prácticas restrictivas o de abuso de posición dominante, y la competencia desleal, garantizando la seguridad nacional, y promoviendo la eficiencia, universalidad, accesibilidad, continuidad y la calidad del servicio[21].

Las entidades públicas encargadas del sector relacionado a las TICs fueron: el Consejo Nacional de Telecomunicaciones (CONATEL) y la Secretaría Nacional de Telecomunicaciones (SENATEL). A partir de su creación, el CONATEL tenía competencias relacionadas al manejo del sector de las telecomunicaciones en el Ecuador. Esta institución fue la encargada de establecer, principalmente, las políticas, planes y normas de las telecomunicaciones. Ahora bien, mientras el CONATEL cumplía el rol de un órgano administrativo y regulador, la Secretaría Nacional de Telecomunicaciones se creó con el fin de ejecutar la política pública en los ámbitos de su competencia. Es decir que, la SENATEL fungía como la institución pública que materializaba lo propuesto por el CONATEL[22].

A través de sus instituciones, y durante el 2000, el Ecuador buscó fortalecer la institucionalidad del sector público y la gobernabilidad del país por medio de la protección de

[20] Ley No 17930. Presupuesto nacional de sueldos gastos e inversiones. Ejercicio 2005 – 2009. Publicada D.O. 23/12/2005
[21] Ley No. 4. Ley para la transformación económica del Ecuador. Registro oficial 34. 13 de marzo del 2000
[22] Ley 184. Ley Especial de Telecomunicaciones. Registro oficial 996. 10 de agosto de 1992.

los derechos de todos los actores involucrados en el ámbito de las telecomunicaciones. Al mismo tiempo, se promocionaba el uso de las tecnologías como un mecanismo de desarrollo económico (Noboa 2000). Los objetivos del Ecuador en el marco de las estrategias previamente señaladas aportaron el crecimiento del espacio cibernético e, indiscutiblemente a la creación de una nueva necesidad de seguridad. En consideración a esta realidad, el Ecuador promulgó en el 2002 su primera ley relacionada específicamente a la interacción social en el espacio cibernético y la seguridad inherente a dicha interacción.

La "Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos" es el acercamiento más tangible del Ecuador a la seguridad cibernética, antes del 2007. Este cuerpo normativo se elaboró y promulgó debido a la importancia que adquirieron las redes y sistemas de información en el desarrollo del país. Tiene como objeto la regulación de "los mensajes de datos, la firma electrónica, los servicios de certificación, la contratación electrónica y telemática, la prestación de servicios electrónicos, a través de redes de información, incluido el comercio electrónico […]"[23]. Esta ley considera, además, como parte de su objeto la protección de quien accede a los sistemas mencionados.

Las disposiciones específicas sobre seguridad cibernética que abarca esta ley están relacionadas al acceso ilícito en los sistemas, la interferencia de datos o en el sistema, el abuso de dispositivos y el fraude informático. La ley específica cada una de ellas con el fin de reformar el Código Penal del Ecuador vigente en ese entonces. Estas disposiciones fueron reformadas, sin embargo, la ley conservo principios que fomentarían políticas de seguridad cibernética. Entre esos se encuentra la confidencialidad y reserva. Según la Ley, "toda violación a estos principios, principalmente aquellas referidas a la intrusión electrónica, transferencia ilegal de mensajes de datos o violación del secreto profesional, será sancionada conforme a lo dispuesto en esta Ley y demás normas que rigen la materia"[24].

Ahora bien, un elemento más que influyó en el contexto y en el proceso securitizador, no solo de Ecuador sino también de Uruguay, es la posición de estos países en el ámbito

[23] Ley 67. Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos. Registro oficial 557. 17 de abril de 2002
[24] Ley 67. Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos. Registro oficial 557. 17 de abril de 2002

internacional. Por lo que, resulta relevante abordar la influencia de actores externos en el proceso securitizador y las relaciones de poder sobre los Estados que se analizan.

3.2. Relaciones de poder en la securitización del espacio cibernético

Las relaciones de poder entre los actores securitizadores, en este caso, actores nacionales e internacionales, afectan de manera considerable al proceso de la securitización del espacio cibernético. El poder de alguno de los actores, o su influencia sobre otros actores del proceso, tiene una proporcionalidad directa a la capacidad securitizadora del discurso. En esta sección se abordarán las relaciones de poder de Ecuador y Uruguay en el ámbito internacional. Es necesario resaltar que los actores internacionales que han influenciado en los aspectos nacionales de los países de análisis son, en los dos casos, similares. Por lo tanto, en esta sección no se dividirán los casos empíricos, sino que los trataremos en conjunto. Asimismo, esto permitirá *a posteriori*, una mejor comparación de la influencia de los actores internacionales sobre Ecuador y Uruguay.

Entre los actores que podrían ejercer influencia, debido a sus relaciones de poder con los actores securitizadores a nivel nacional, se encuentran los organismos internacionales. Desde organismos de gran magnitud, como las Naciones Unidas, hasta organismos con pequeño número de miembros, como la Unión de Naciones del Sur (UNASUR), han abordado el tema de la seguridad cibernética. Sin embargo, la Organización de los Estados Americanos ha sido el organismo internacional que mayor influencia ha ejercido sobre los países de la región, en temas de seguridad cibernética. Esto se debe, no solo por su cercanía con los Estados miembros como Ecuador y Uruguay, sino por el desarrollo de prácticas internacionales que impulsan el proceso de securitización del espacio cibernético de los países.

3.2.1. La Organización de los Estados Americanos

A través de varias de sus unidades, la OEA ha abordado el tema de los ataques cibernéticos como una prioridad de diálogo entre los Estados miembros con el fin de implementar las acciones de respuesta necesarias. Como parte de esta organización, las unidades que han liderado este proceso son: la Comisión Interamericana de Telecomunicaciones (CITEL), el Grupo de Expertos Gubernamentales en Materia de Delito Cibernético y, principalmente, el Comité Interamericano contra el Terrorismo (CICTE). Cada uno de ellos ha aportado en la influencia de la OEA en los países que la conforman.

El CICTE, en su sexta sesión plenaria adoptó la "Declaración de San Salvador sobre el Fortalecimiento de la Cooperación en la Lucha contra el Terrorismo". Esta declaración fue uno de los primeros elementos discursivos más claros sobre el impulso de la seguridad cibernética. En ella se establece que "las amenazas emergentes del terrorismo, tales como las actividades de grupos terroristas internacionales y las amenazas a la seguridad cibernética, exigen un diálogo permanente entre los Estados Miembros a fin de adoptar medidas preventivas eficaces para anticiparlos y abordarlos"[25].

El discurso securitizador del espacio cibernético nacional, se fortaleció a través de las declaraciones de la Asamblea General de la OEA por medio de sus resoluciones AG/RES. 1939 (XXXIII-O/03) y AG/RES. 2004 (XXXIV-O/04). En la primera resolución se impulsa la creación de una estrategia sobre seguridad cibernética. Esta estrategia sería desarrollada por la Comisión de Seguridad Hemisférica de la OEA y debería integrar "aspectos multidimensional y multidisciplinario de la seguridad cibernética"[26]. Por medio de la segunda resolución mencionada previamente, la Asamblea General aprobó la "Estrategia Interamericana Integral de Seguridad Cibernética: Un enfoque multidimensional y multidisciplinario para la creación de una cultura de seguridad cibernética". De igual manera, exhortó a todos los países miembros a implementar dicha estrategia en el ámbito nacional y a fomentar

> una cultura de seguridad cibernética en las Américas adoptando medidas de prevención eficaces para prever, tratar y responder a los ataques cibernéticos, cualquiera sea su origen, luchando contra las amenazas cibernéticas y la delincuencia cibernética, tipificando los ataques contra el espacio cibernético, protegiendo la infraestructura crítica y asegurando las redes de los sistemas[27].

Otro de los principales instrumentos discursivos de la OEA es la declaración para el "Fortalecimiento de la Seguridad Cibernética en las Américas". Aprobada en el 2012 por el CICTE, esta declaración busca reiterar la responsabilidad de los Estados miembros de cumplir, a nivel nacional, con las estrategias propuestas por el Comité en temas de seguridad

[25] OEA/Ser.L/X.2.3 CICTE/DEC.1/03 rev. 2 Declaración de San Salvador sobre el Fortalecimiento de la Cooperación en la Lucha contra el Terrorismo. 29 de enero de 2003
[26] AG/RES. 1939 (XXXIII-O/03) Desarrollo de una estrategia interamericana para combatir las amenazas a la seguridad cibernética. 10 de junio de 2003
[27] OEA. Resolución AG/RES.2004 (XXXIV-0/04). Estrategia Interamericana Integral de Seguridad Cibernética: Un Enfoque Multidimensional y Multidisciplinario para la creación de una cultura de seguridad cibernética. 4ta sesión, julio 2004.

cibernética. El Comité declara en este documento "su voluntad de continuar desarrollando estrategias nacionales de seguridad cibernética integrales e involucrar a todos los actores pertinentes en su desarrollo e implementación"[28].

3.2.2. Estados Unidos de Norteamérica

Un país que debe ser analizado con relación a las relaciones de poder, es los Estados Unidos. El rol de este Estado en el sistema internacional le permite ejercer una importante influencia en los procesos securitizadores del resto de países, en especial de países de América del Sur como Ecuador y Uruguay. El discurso y prácticas de seguridad cibernética adoptadas por este país habrían impulsado el proceso de securitización del espacio cibernético alrededor del mundo. Por estos motivos, se analizarán las principales herramientas discursivas y prácticas que promovieron a la securitización de las TICs y del ciberespacio.

El impulso más importante a la búsqueda del desarrollo de agendas de seguridad cibernética en el resto de países por parte de Estados Unidos, podría tener como hito, la creación de la Oficina del Coordinador de Asuntos Cibernéticos en 2011. Esta oficina está encargada, entre otras atribuciones, de coordinar la inserción diplomática de los asuntos cibernéticos y coordinar el trabajo con las instancias estadounidenses del Departamento de Estado encargadas del trabajo en diferentes regiones del mundo. Las competencias que forman la base de la oficina de asuntos cibernéticos son la promoción de TICs relacionadas al aspecto comercial que funcionen de manera segura y confiable; y, el fortalecimiento de la seguridad internacional (U.S. State Department 2017).

En 2011, el gobierno de Estados Unidos estableció una Estratégica Internacional de Política para el Ciberespacio que abarca varios ámbitos: economía digital, seguridad internacional, debida diligencia en la promoción de la ciberseguridad, combate el crimen cibernético, gobernanza del internet, libertad, desarrollo internacional y creación de capacidades. Esta estrategia fue renovada en 2016 conservando sus fundamentos básicos (White House 2011).

En todos estos ámbitos, Estados Unidos ha ejercido una influencia internacional, incluidos países como Ecuador y Uruguay. Las relaciones de poder le permiten "liderar y moldear el

[28] OEA/Ser.L/X.2.12 CICTE/DEC.1/12 rev.1 Declaración "Fortalecimiento de la Seguridad Cibernética en las Américas" 7 de marzo de 2012

debate internacional[29]" (Department of State 2016, 2). Profundizando en la estrategia y las relaciones de poder, se resaltan los esfuerzos de Estados Unidos para crear capacidad y fomentar el desarrollo de políticas de seguridad cibernética, especialmente en regiones clave como América Latina (Department of State 2016).

De igual manera, Estados Unidos consolidó política exterior especializada para la temática. La denominó Ciber Diplomacia. Sus objetivos se enfocan en la concientización del entendimiento común de las problemáticas del ciberespacio, impulsar la seguridad cibernética, el estado de derecho internacional en este escenario y reducir el riesgo en el uso de las TICs.

> Los Estados deben promover estabilidad internacional, transparencia y confianza en el ciberespacio; leyes internacionales existentes son aplicables al comportamiento del Estado en relación al uso del ciberespacio; y la comunidad internacional debería ayuda a la creación de capacidades de los países menos desarrollados (Office of the Coordinator For Cyber Issues 2015, 1-2).

3.3. Instrumentos de seguridad cibernética

3.3.1. Principales instrumentos de seguridad cibernética en Uruguay

Si bien Uruguay no cuenta con una agenda de seguridad cibernética específica, ni un documento de política pública que enmarque el accionar del país en este ámbito; el gobierno uruguayo ha introducido mecanismos de seguridad cibernética en su ordenamiento normativo interno. Además, a través de la AGESIC, ha impulsado lineamientos de seguridad enfocados en el ámbito cibernético por medio de otras agendas de gobierno que abarcan temáticas relacionadas al espacio digital y la información.

El Código Penal de Uruguay incorpora en su cuerpo normativo un artículo determinado sobre seguridad cibernética, específicamente, establece penas para quien afecte el servicio de telecomunicación. El artículo 217 establece que:

> El que, de cualquier manera, atentare contra la regularidad de las telecomunicaciones alámbricas o inalámbricas, será castigado con tres meses de prisión a tres años de penitenciaría. Se considera agravante especial de este delito, la sustracción, el daño o la

[29] Traducción: autor

> destrucción de instalaciones destinadas a las prestaciones del servicio de telecomunicaciones[30].

De igual manera, el ordenamiento normativo ha establecido obligatoriedad para las instituciones del Estado uruguayo para que adopten políticas de seguridad de la información que se encuentra en el espacio cibernético[31]. En base a esta obligatoriedad, el Consejo Directivo de la AGESIC difundió, en el 2010, la resolución CDH 62/010, por medio de la cual resuelve difundir "[…] la Política de Gestión de Incidentes de Seguridad de la Información y la Política de Gestión del Riesgo de Seguridad de la Información a todos los organismos de la Administración Pública, otorgándoles un plazo de 180 días para su adopción"[32].

Otros mecanismos normativos de Uruguay se han enfocado en la protección de la información, específicamente, la protección de datos personales. La Constitución de Uruguay otorga como un derecho humano, la protección de datos personales. En concordancia con este derecho, se emitió la Ley de "Protección de datos personales y acción de habeas data", la cual amplia el derecho a personas jurídicas. Por medio de esta ley, se establecen datos sensibles que deben ser protegidos a través de mecanismos especiales. Sobre la información en las telecomunicaciones, la importancia de lo que establece esta ley motiva a transcribir el artículo en su integridad.

> Los operadores que exploten redes públicas o que presten servicios de comunicaciones electrónicas disponibles al público deberán garantizar, en el ejercicio de su actividad, la protección de los datos personales conforme a la presente ley. Asimismo, deberán adoptar las medidas técnicas y de gestiones adecuadas para preservar la seguridad en la explotación de su red o en la prestación de sus servicios, con el fin de garantizar sus niveles de protección de los datos personales que sean exigidos por la normativa de desarrollo de esta ley en esta materia. En caso de que exista un riesgo particular de violación de la seguridad de la red pública de comunicaciones electrónicas, el operador que explote dicha red o preste el servicio de comunicaciones electrónicas informará a los abonados sobre dicho riesgo y sobre las medidas a adoptar. La regulación contenida en esta ley se entiende sin perjuicio de lo previsto en la

[30] Código Penal. Febrero de 2004
[31] Decreto 451/009. Administración pública. Política de seguridad de la información. 28 de septiembre de 2009.
[32] No. 2 de la Resolución CDH 62/010. Consejo Directivo Honorario de la AGESIC. 13 de octubre de 2010

> normativa específica sobre telecomunicaciones relacionadas con la seguridad pública y la defensa nacional[33].

A partir de la ley previamente mencionada, Uruguay emitió otros documentos normativos que fortalezcan la protección de datos personales contenidos en el ciberespacio. En el 2009, se expidió el reglamento a la ley de protección de datos personales[34] y en el 2013, se emitió la ley que aprobó el "Convenio N° 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal[35]" y su protocolo. La ley menciona que "se tomarán medidas de seguridad apropiadas para la protección de datos de carácter personal registrados en ficheros automatizados contra la destrucción accidental o no autorizada, o la pérdida accidental, así como contra el acceso, la modificación o la difusión no autorizados"[36].

Ahora bien, además del ordenamiento normativo la AGESIC mantiene uno de los pilares encaminados a garantizar la seguridad ciudadana y el uso confiable de las tecnologías de la información y la comunicación. Para dar cumplimiento a este fin, el gobierno ha creado un marco regulatorio que norma el uso de las TIC y la protección de información para garantizar la seguridad de la población. Además, por medio de la AGESIC, el gobierno ha impulsado la instauración de infraestructura necesaria para dar cumplimiento a lo determinado en sus políticas públicas. Como parte de la iniciativa de seguridad y confianza, la AGESIC menciona que ha creado

> la infraestructura crítica y el marco regulatorio habilitante necesario para que la ciudadanía tenga seguridad y confianza en el uso de las TIC. Para ello, [desarrollaron] el Centro Nacional de Respuestas a Incidentes en Seguridad Informática (CERTuy), infraestructura nacional en certificación electrónica, identidad electrónica, al mismo tiempo [elaboraron] leyes sobre seguridad de la información, privacidad y protección de datos personales (AGESIC 2018).

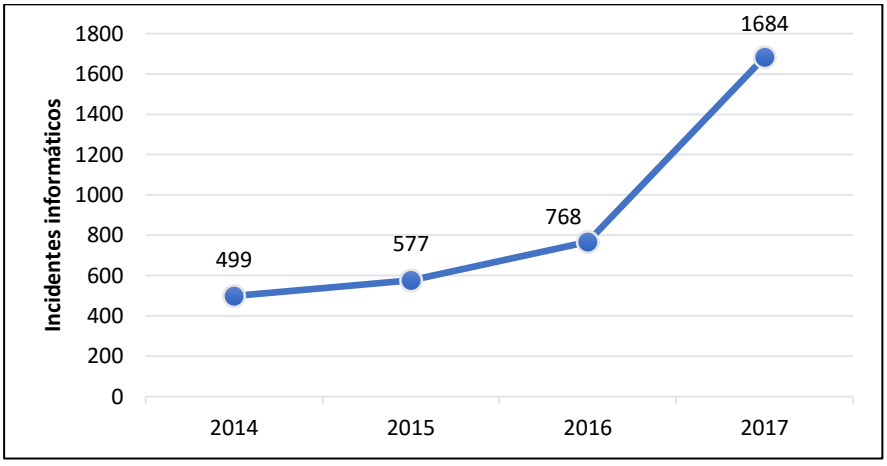
Durante el proceso securitizador, y especialmente en los últimos años de gobierno, los ataques cibernéticos han permitido legitimar la construcción de agendas específicas para la seguridad

[33] Ley No 19.331. Protección de datos personales y acción de "habeas data". 11 de agosto de 2008
[34] Decreto No. 414/009. protección de datos personales – acción de "habeas data" – reglamentación. 31 de agosto de 2009.
[35] Ley No. 19030. Aprobación del convenio 108. 07 de enero de 2013.
[36] Art. 7. Ley No. 19030. Aprobación del convenio 108. 07 de enero de 2013.

cibernética; así como la creación de instrumentos que aborden las amenazas en este ámbito. Desde el 2014, el gobierno uruguayo ha llevado registro de los ataques cibernéticos de los que ha sido objeto. En el 2014, se presentaron 499 incidentes informáticos. Para el siguiente año, en el 2015, los incidentes incrementaron en un 20%; alcanzando un total de 577. Entre todos los incidentes informáticos hasta el 2017, el año 2015 es en el único en el que se ha enfrentado ataques de denegación de servicio (DoS) (AGESIC 2016).

Para el 2016, Uruguay enfrento 33% más ataques informáticos en comparación con el año previo, alcanzando los 768 incidentes. En el 2017 el número de incidentes crece considerablemente, 120%, llegando a los 1684. No obstante, el crecimiento de incidentes no responde únicamente a una mayor cantidad de ataques. A mediados de año el gobierno uruguayo inauguró el Centro de Operaciones de Seguridad (SOC), el cual debido a sus funciones permitió mejor identificación de las amenazas al espacio cibernético (AGESIC 2018). Si bien estas estadísticas permiten visualizar la realidad del espacio cibernético y los incidentes que se presentan, el numérico de casos son aquellos que fueron denunciados y detectados. Por lo tanto, no se ha logrado conocer exactamente la cantidad de casos que se presentan a nivel país en un año.

Gráfico 4: Incidentes informáticos identificados en Uruguay (2014 – 2017)



Fuente: Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento

Por otro lado, en septiembre de 2017, en Uruguay se logró detener a una persona involucrada en un importante ataque a la seguridad cibernética de una institución financiera de carácter privado. La institución fue extorsionada con la devolución de información sensible que fue robada a través de un ataque a su sistema informático. Este fue el primer caso de esta

naturaleza que finalizó con la prisión del atacante. Sin embargo, la mediatización de este evento habría concientizado a la audiencia sobre las amenazas tecnológicas y habría permitido la consolidación de las medidas de seguridad cibernética y la aceptación del discurso securitizador en todo el país (Ministerio del Interior 2017).

Ahora bien, incluso cuando no existen mecanismos que permiten determinar el número exacto de incidentes informáticos a los que se enfrenta Uruguay en un año, las estadísticas y casos específicos aportan a la comprensión del escenario en el que se desenvuelve el discurso securitizador del espacio cibernético. El aumento de incidentes informáticos concuerda con la ampliación de las agendas securitizadoras y la creación de instrumentos de seguridad cibernética. Además, la existencia real de amenazas a los objetos referentes facilita la intersubjetividad, entre todos los actores de la sociedad uruguaya, de la necesidad de contar con medidas extraordinarias para garantizar la seguridad en el espacio cibernético. Es en este escenario en el que se desenvuelven los instrumentos de seguridad informática.

3.3.1.1. Centro Nacional de Respuesta a Incidentes de Seguridad Informática del Uruguay (CERTuy)

Como instrumento de seguridad del espacio cibernético, la presidencia del gobierno uruguayo dispuso, el 6 de octubre de 2008, por medio del Art. 73 de la rendición de cuentas y balance ejecutivo presupuestal del ejercicio 2007, la creación de un "Centro Nacional de Respuesta a Incidentes de Seguridad Informática (CERTuy)". Este centro es parte de la AGESIC[37]. Aporta en la seguridad ciudadana, la protección de información y la promulgación de cultura para la seguridad de la información. Los principales objetivos de esta institución son: "centralizar, coordinar y optimizar los procesos de respuesta a incidentes en seguridad de la información; difundir mejores prácticas en seguridad de la información y realizar tareas preventivas" (CERTuy 2018).

Este centro ha establecido como su misión prioritaria la protección de la información crítica del Estado, focalizando sus actuaciones de prevención y respuesta a amenazas de instituciones específicas. Por lo que deja, en su gran mayoría, la seguridad cibernética de otros actores bajo su responsabilidad. El ámbito objetivo del CERTuy, establecido por el gobierno uruguayo en el 2009, es la protección de "los sistemas informáticos que soporten activos de información

[37] Ley No 18.362. Rendición de cuentas y balance de ejecución presupuestal ejercicio 2017. Publicada D.O. 15 oct/2008 – No 27590

críticos del Estado, así como los sistemas circundantes a éstos".[38] Los ámbitos para los que trabajo este centro son: "gobierno, salud, orden público, servicios de emergencia, energía, telecomunicaciones, transporte, suministro de agua potable, ecología y ambiente, agro-industria, banca y servicios financieros" (CERTuy 2018), así como, cualquier ámbito en el que se vea afectada más del 30% de la población. Las potestades del centro lo convierten en el principal instrumento para la seguridad informática de la infraestructura crítica y de las instituciones del Estado uruguayo.

Con base a las actividades realizadas por el CERTuy, se presentó la necesidad de incrementar los instrumentos estatales que permitan hacer frente a las amenazas informáticas. Para fortalecer la seguridad cibernética de Uruguay, el gobierno liderado por el presidente José Mujica con el apoyo del ministro Eleuterio Fernández Huidobro, el 27 de enero de 2015, instauró una oficina específica para la prevención y atención de posibles ataques cibernéticos como parte del Ministerio de Defensa Nacional. Por medio de un decreto presidencial, se creó el "Centro de Respuesta a Incidentes de Seguridad Informática (D-CSIRT)" (Presidencia de la República de Uruguay 2015).

3.3.1.2. Centro de Respuesta a Incidentes de Seguridad Informática (D- CSIRT)

Este centro del Ministerio de Defensa se dedica únicamente a la seguridad cibernética de las unidades y dependencias de este ministerio. El D-CSIRT es el coordinador de todas las actividades que se ejecuten en esta instancia, relacionada a incidentes de seguridad informática. Su principal objetico busca la participación "de forma eficaz y eficiente en la respuesta a incidentes informáticos sobre infraestructuras críticas y servicios esenciales [de las unidades y dependencias del Ministerio de Defensa], así como desarrollar capacidades de prevención y detección temprana de incidentes de seguridad informática de dicha comunidad"[39]. Los límites de actuación de esta unidad se alinean con una visión tradicional de seguridad, enfocada en la defensa del Estado.

Sin embargo, la materialización del discurso securitizador en este tipo de herramientas, ha creado la necesidad de cooperación intra institucional entre las dependencias del gobierno

[38] Art. 1 del Decreto No 451/009. Centro de Respuesta a Incidentes de Seguridad Informática. Funcionamiento y Organización. Publicado D.O. 08/10/2009

[39] Decreto No 36/2015. Creación del Centro de Respuesta a Incidentes de Seguridad Informática en el Ministerio de Defensa Nacional (D-CSIRT). Publicado D.O. 20/02/2015

uruguayo. Por lo tanto, si bien el D-CSIRT forma parte del Ministerio de Defensa, debe colaborar de manera activa con el centro nacional CERTuy y, en un ámbito de mayor carácter político, con la AGESIC. Además, el D-CSIRT tiene como lineamiento implementar las regulaciones emitidas por el centro nacional[40]. Para un funcionamiento eficiente de estas dos unidades que permitieron la descentralizaron de actividades estatales direccionadas hacia la seguridad cibernética, se requiere un alto nivel de coordinación. No solo para la promulgación de política de seguridad nacional, sino también, para la cooperación con instituciones internacionales.

3.3.2. Principales instrumentos de seguridad cibernética en Ecuador

En el Ecuador, el ordenamiento normativo también ha introducido mecanismos de seguridad cibernética, como resultados mediatos del proceso securitizador. En concordancia con la normativa mencionada en el contexto, específicamente la Ley de Comercio Electrónico, el Código Orgánico Integral Penal (COIP) ha incorporado artículos que sancionan las afectaciones de un ataque cibernético. En protección del derecho a la intimidad, el COIP sanciona a cualquier persona que "sin contar con el consentimiento o la autorización legal, acceda, intercepte, examine, retenga, grabe, reproduzca, difunda o publique datos personales, mensajes de datos, voz, audio y vídeo, objetos postales, información contenida en soportes informáticos, comunicaciones privadas o reservadas de otra persona por cualquier medio"[41].

Además de algunos delitos que han considerado el escenario informático, el Código Penal de Ecuador ha incorporado una sección denominada "Delitos contra la seguridad de los activos de los sistemas de información y comunicación"[42]. En esta sección se han tipificado seis tipos delictivos: la revelación ilegal de una base de datos, la interceptación ilegal, la transferencia o apropiación no consentida de un patrimonio electrónico, el ataque a sistemas, delitos contra la información de carácter público y el acceso no consentido a sistemas informáticos. La inserción de estos temas representa un importante avance en temas de seguridad cibernética.

Ahora bien, uno de los instrumentos por los cuales el Ecuador se desenvuelve en el ámbito de la seguridad cibernética, es el Centro de Repuesta a Incidentes Informáticos del Ecuador

[40] Decreto No 36/2015. Creación del Centro de Respuesta a Incidentes de Seguridad Informática en el Ministerio de Defensa Nacional (D-CSIRT). Publicado D.O. 20/02/2015
[41] Código Orgánico Integral Penal. Registro oficial 180. 10 de febrero de 2014.
[42] Sección Tercera. Art. 229. Código Orgánico Integral Penal. Registro oficial 180. 10 de febrero de 2014.

(ecucert). El Centro empezó a funcionar desde noviembre de 2013. Este centro es parte de la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL). El ecucert trabaja para

> masificar el uso de Internet, las tecnologías de la información y los sistemas de telecomunicaciones en todo nuestro país, mediante la coordinación, nacional e internacional de acciones técnicas destinadas a lograr usos más seguros de las redes, que satisfagan la confianza de la comunidad que las utiliza (ecucert 2017, 1).

El ecucert tiene como misión "brindar a su comunidad objetivo el apoyo en la prevención y resolución de incidentes de seguridad informática, a través de la coordinación, capacitación y soporte técnico". La comunidad objetivo del centro de respuesta es, la ARCOTEL, todas las instituciones que ofertan servicios de telecomunicación y las instituciones del sector público y privado que han solicitado los servicios del ecucert. Uno de los principales objetivos del centro es "garantizar la seguridad de los servicios de telecomunicación, la información transmitida y la vulnerabilidad de la red". Este objetivo se enfoca en la comunidad objetivo y se lo articula con los miembros que la integran. Además, tienen el propósito de controlar a entidades públicas y privadas para que se incorporen medidas de seguridad cibernética adecuadas en términos de equipamientos tecnológico y gestión.

El ecucert también tiene como objetivo impulsar buenas prácticas de uso de las tecnologías de la información y la comunicación en todos los ámbitos de la sociedad ecuatoriana. Para cumplir con este objetivo, busca implementar mecanismos específicos de coordinación a través de un Comité de Ciberseguridad que "desarrollará y promoverá guías de buenas prácticas y recomendaciones en seguridad de la información" (ecucert 2017, 1).

Otra herramienta adoptada por Ecuador para hacer frente a los riesgos y amenazas cibernéticas es el Comando de Ciberdefensa de las Fuerzas Armadas. Esta unidad militar fue creada en septiembre de 2004 mediante Acuerdo Ministerial 281. Sus actividades de defensa se enfocan primordialmente en la protección de la infraestructura e información crítica del Estado. Si bien, esta herramienta puede ser considerada como un resultado del discurso securitizador, su enfoque se basa en la defensa de la soberanía digital por lo que no abarca en gran medida la seguridad de la sociedad en su interacción en el espacio cibernético.

3.4. Ecuador y Uruguay: semejanzas y diferencias de los factores externos del discurso securitizador

El análisis del contexto histórico de discurso securitizador tanto en Ecuador como en Uruguay permite observar las amplias diferencias del proceso en los dos países. Un hecho relevante que es necesario resaltar, es que, si bien Ecuador fue uno de los países pioneros en incorporarse a la red y al internet en Sudamérica, una década después era de los países con menor desarrollo de las tecnologías de la información y comunicación en la región. Esta diferencia histórica, ya marca un hito importante que influencia en el proceso securitizador del espacio cibernético entre los dos países. No obstante, la temporalidad en la que se generan las bases para la construcción de una agenda de seguridad cibernética no es distante entre un país y otro. Se identifico que, en el año 2000, Ecuador y Uruguay proponían al espacio cibernético como una herramienta gubernamental que permitiría mejorar el servicio que las instituciones públicas ofrecían a la ciudadanía.

El impulso del uso de las TICs en el manejo gubernamental constituye la base de los procesos de construcción del discurso securitizador del espacio cibernético en los dos países de análisis. La necesidad de evitar o disminuir los riesgos del uso de la tecnología y la red, así como la protección de la información, en las instituciones públicas motivó el inicio de las agendas de seguridad cibernética. Si bien las motivaciones fueron semejantes, la consolidación de instituciones encargadas de estos temas fue diferente en Uruguay y Ecuador. Es así como mientras en Uruguay se creó a la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y el Conocimiento (AGESIC) en el 2005, en Ecuador no se lograba la creación de una institución única, responsable. Y hasta el 2013, durante el proceso discursivo securitizador del espacio cibernético, se otorgaron las responsabilidades al Ministerio de Telecomunicaciones y a la Agencia de Control, ARCOTEL.

Como un segundo factor, las relaciones de poder de actores externos sobre los países de análisis son semejantes. Tanto la Organización de los Estados Americanos, como los diferentes gobiernos de los Estados Unidos de Norteamérica, han manejado agendas de influencia discursiva para la seguridad del espacio cibernético en los países de la región, entre esos países, Ecuador y Uruguay. En el caso de los actores internacionales analizados, tanto la OEA, como EE. UU. debido a su posición en temas relacionados a la seguridad, introdujeron a la seguridad cibernética como un área que debe ser tratada a nivel nacional. Esto, no solo

con el fin de garantizar la seguridad nacional sino, además, para fortalecer la posición de estos actores en el sistema internacional.

La OEA al ser un organismo internacional, influenció a los actores securitizadores de carácter nacional de una manera diferente a un país como Estados Unidos. La OEA difundido documentos internacionales que exhortan a los países de la región a securitizar el espacio cibernético. Este organismo internacional, no solo impulsa el establecimiento del discurso securitizador. También propone estrategias determinadas para la securitización práctica del ciberespacio. Estados Unidos, por su parte, al ser un país más de la región, ejerce su influencia de manera diferente. Los gobiernos de este país han hecho uso de las herramientas diplomáticas y de las unidades relacionadas al Departamento de Estado, para fomentar el discurso securitizador a nivel internacional.

El último factor externo y de comparación entre Ecuador y Uruguay, es el referente a las prácticas e instrumentos que impulsan el proceso de construcción de agendas de seguridad cibernética, pero que, además, son resultados mediatos del discurso securitizador. Las prácticas e instrumentos de Ecuador y Uruguay fueron creados como resultado del inicio del proceso intersubjetivo de creación de medidas de seguridad cibernética. En los dos países de análisis, se ha enfocado la atención en las instituciones que abordan temas de seguridad cibernética y en la manera en cómo funcionan. Es así como se puede determinar una semejanza, tanto Ecuador como Uruguay han creado instituciones que abordan temas de seguridad cibernética y que, en mayor o menor medida, apoyan a la consolidación del discurso securitizador del espacio cibernético y del uso de las TICs.

En Uruguay, las practicas e instrumentos se enmarcan en el funcionamiento de la AGESIC. Se han creado centros encargados de la seguridad cibernética como el CERTuy o el D-CSIRT. Cada uno de estos centros aportan a la seguridad del espacio cibernético de Uruguay. Están a cargo de la construcción de una cultura de seguridad de la información, de la actuación frente ataques cibernéticos, de actuaciones de prevención y en la protección de la infraestructura crítica y de las instituciones gubernamentales. Las prácticas de estas instituciones, al involucrarse en varios ámbitos de la sociedad, han aportado a los actores securitizadores a ejercer una mayor influencia en la audiencia para la consolidación de una agenda de seguridad cibernética. Estas instituciones demuestran mayor consolidación y mejor alcance de sus prácticas, en comparación con las herramientas del gobierno ecuatoriano.

A diferencia de la creación del primer centro de respuesta a incidentes informáticos de Uruguay en 2007, el centro de respuesta de ecuador empezó a funcionar en 2013. El Ecucert impulsa acciones relacionadas a la difusión del uso del internet, a la seguridad del ciberespacio, a la protección de la información y al impulso de actores públicos y privados de incorporar protocolos de seguridad cibernética en sus prácticas cotidianas. Forma parte, además, de un Comité de Ciberseguridad que se enfocó en la promoción de buenas prácticas para garantizar la seguridad de la información en las instituciones públicas. Si bien estas instituciones han aportado al proceso de construcción de una agenda de ciberseguridad en Ecuador, fundamentalmente han enfocado sus esfuerzos en el sector público y no han aportado, en mayor medida, en la difusión del discurso a la audiencia en general.

Conclusiones

La seguridad cibernética es una respuesta a los riesgos y amenazas del desarrollo tecnológico, la expansión del internet y la incursión de equipos tecnológicos en las actividades cotidianas de la sociedad. Alrededor del mundo se han impulsado respuestas que permitan asegurar el uso de las tecnologías de la información y la comunicación, así como medidas que garanticen la información que está tecnología contiene. Los varios actores internacionales han demostrado su interés en el impulso de agendas de seguridad y defensa cibernética. Si bien éste continúa siendo un tema de investigación y análisis, la presente investigación no abordó de manera extensa la construcción de seguridad cibernética en términos militares en los casos empíricos. Esto se debe a que la motivación de mecanismos de defensa cibernética responde a garantizar la sobrevivencia del Estado, es decir que, la defensa cibernética es vino viejo en botellas nuevas.

Ahora bien, en términos de seguridad interna, es importante resaltar que las agendas de ciberseguridad son construidas a través de procesos de securitización en los que participan una gran variedad de actores. Como se ha visualizado a lo largo de la investigación, la securitización ha involucrado al gobierno, a diversos grupos de la sociedad, a organismos internacionales y otros países ajenos a la región. Todos estos actores se han difuminado entre un rol securitizador y un rol de agencia. Sin embargo, la interacción social entre todos ellos y la interacción con su alter, quien debido a sus intereses genera amenazas y riesgos en el espacio cibernético, crea las necesidades de seguridad cibernética.

Los casos de estudio seleccionados dentro de la región latinoamericana permiten analizar de mejor manera las diferencias que han motivado un mayor desarrollo del proceso de securitización para el establecimiento de una agenda de seguridad cibernética en un país determinado frente a otro. En concordancia con el método, la selección de países símiles como Ecuador y Uruguay permitió la determinación de diferencias en la construcción de agendas de seguridad cibernética. Como se mencionó al inicio de la investigación, Ecuador y Uruguay son países similares, en términos generales. Sin embargo, a pesar de que Ecuador es uno de los países que mayor cantidad de ataques cibernéticos ha enfrentado, no ha logrado avances relevantes en seguridad cibernética. Uruguay, por su lado, es uno de los países pioneros en ciberseguridad. Las causas de esta diferencia están inmersas en los factores provenientes de la teoría de la securitización.

La complejidad que presenta un nuevo escenario de interacción social de alcance mundial dificulta la investigación sobre un ámbito específico como la seguridad. Por este motivo, bajo el supuesto que la seguridad es un proceso de construcción intersubjetivo, la teoría de la securitización ha aportado con los elementos teóricos apropiados para el análisis de la seguridad cibernética en Ecuador y Uruguay. Si bien su posición clásica, alineada a los supuestos presentados por Buzan y la Escuela de Copenhague es adecuada para analizar el discurso en sí; los supuestos teóricos presentados por Balzacq han sido considerados como elementos importantes que aportan y completan el análisis. Por este motivo, la investigación consideró dos tipos de factores a ser analizados. En primer lugar, los factores internos o factores lingüísticos de la securitización: el objeto referente la audiencia y el actor securitizador. Posteriormente se consideraron los factores externos: el contexto, las relaciones de poder y las prácticas e instrumentos.

Así, el análisis de los factores lingüísticos y factores externos que han sido promovidos por varios académicos que han empleado la teoría de la securitización, permite una posición ontológica y epistemológica adecuada para explicar la construcción de las agendas de seguridad cibernética en Ecuador y Uruguay, y poder compararlas. El abordaje de los dos grupos de factores permite entender el proceso intersubjetivo del discurso securitizador, sin discriminar las influencias externas a las que es objeto y que, en gran medida, afectan su efectividad al momento de establecer medidas de seguridad sobre el objeto referente.

La posición teórica mencionada previamente ha permitido la determinación de elementos que permiten explicar las diferencias en la construcción de agendas de securitización del espacio cibernético en Ecuador y Uruguay, a través del método de la diferencia propuesto por Stuart Mill. Especialmente, los motivos por los cuales, a pesar de tener características macro similares y haber sido objeto de ataques cibernéticos de relevancia, el discurso securitizador en Uruguay tiene un mayor avance en comparación de Ecuador. Un mayor alcance de, tanto los factores internos como externos, en Uruguay comparado con Ecuador, han permitido la comprensión de las diferencias de este proceso en términos empíricos.

Los factores lingüísticos presentan ciertas similitudes en los dos países. Sin embargo, cuando se involucran los factores externos, se logra comprender la diferencia entre un Estado y otro. En primer lugar, el objeto referente es semejante, la seguridad busca la protección del espacio

cibernético frente a los riesgos y amenazas de las que puede ser objeto. Ahora bien, esta similitud se distorsiona al determinar la relevancia que tiene para un país y para otro el espacio cibernético. Es en este momento que la explicación del contexto histórico nos permite comprender porque el objeto referente, con relación a la seguridad cibernética, tiene una mayor dimensión. El impulso de Uruguay al desarrollo de las tecnologías de la información y la comunicación hizo que la sociedad uruguaya, mucho antes que Ecuador, tenga acceso al uso de las redes, del internet y en la interacción en el ciberespacio.

Una diferencia que se ha considerado como fundamental con relación al objeto referente, es su correlación con los actores de la sociedad en los casos de análisis. Mientras Uruguay ha impulsado la inserción de las tecnologías de la información y comunicación en todos los ámbitos de la sociedad, promoviendo la participación de la ciudadanía en el espacio cibernético y, por lo tanto, acercando el objeto referente a las prácticas cotidianas de la sociedad; Ecuador se enfocó en sus instituciones públicas. El gobierno ecuatoriano impulsó el desarrollo de las tecnologías de la información y comunicación como una herramienta que permitiese mejorar el servicio que brindan las instituciones públicas a la ciudadanía.

Uno de los aciertos del discurso difundido por los actores securitizadores uruguayos se basa en la concientización de las afectaciones de un ataque cibernético a las garantías básicas de la audiencia. Las instituciones uruguayas, desde el 2008, han promovido la seguridad cibernética en el ámbito de la salud. La promoción de la importancia de la protección de la información médica y de los equipos tecnológicos ha sido una constante. La ampliación del objeto referente, no solo en la información y en el uso de las redes sociales, ha permitido que la sociedad uruguaya aporte de manera más significativa a la construcción de una agenda de ciberseguridad y a la instauración de prácticas excepcionales en el manejo de la información y de la tecnología.

Ahora bien, una mayor población involucrada con el ciberespacio, también se convierte en una población más consciente de los riesgos y amenazas a los que se enfrenta. La audiencia del proceso intersubjetivo está más presta a aceptar el discurso securitizador y a la implementación de medidas extraordinarias. Cuando analizamos a la audiencia en Ecuador y Uruguay, ya se mencionó que la sociedad uruguaya conoce los riesgos y amenazas del espacio cibernético, e incluso ha aportado al discurso de los actores securitizadores. Ecuador por su lado, tiene una sociedad que interactúa en el espacio cibernético, pero no implementa

medidas de seguridad, por falta de conocimiento de los riegos o amenazas de la red, o porque el discurso securitizador no ha logrado calar en la población que es consciente de los riesgos, limitando la intersubjetividad en la construcción de agendas de ciberseguridad.

No obstante, la difusión del discurso securitizador por varios mecanismos en Ecuador, la sociedad no tiene un amplio conocimiento de las medias de seguridad cibernética que el gobierno ecuatoriano busca impulsar. Es así como, la agenda de seguridad cibernética y las medidas extraordinarias que se derivan de ella, se han implementado en las instituciones públicas, más no en las privadas y en la población en general. En Uruguay, la integralidad del discurso securitizador ha permitido que la audiencia acepte las medidas propuestas. Por otro lado, el mismo contexto histórico que impulsó el crecimiento del espacio cibernético en mayor medida en Uruguay, permitió que el discurso securitizador inicie previamente en comparación con Ecuador.

Con relación a los factores externos, el contexto ha sido una de las razones base para la diferencia en la construcción de agendas de los dos países. Este factor es trasversal al comportamiento del resto de factores analizados. Sin embargo, es importante resaltar que el impulsó previo al desarrollo de las tecnologías de la información y la comunicación en Uruguay, en comparación con Ecuador, creó la necesidad de empezar a pensar en seguridad cibernética. A pesar de que Ecuador fue uno de los primeros países en impulsar la interacción en el espacio cibernético; Uruguay presenta un mayor desarrollo tecnológico. En el contexto externo, al analizar las relaciones de poder de actores internacionales sobre Ecuador y Uruguay, se han encontrado similitudes que fortalece el análisis comparado entre estos países.

En consideración de las relaciones de poder, las condiciones internacionales no son las que han determinado un mayor desarrollo del proceso de seguridad cibernética en Uruguay en comparación con Ecuador. Los dos países han mantenido una posición similar en el marco de organismos internacionales y han respondido de manera similar a Estados Unidos, como un país influyente en el contexto internacional. La promoción de las agendas internacionales de seguridad cibernética ha servido a los dos países como direccionamientos para la construcción interna de sus agendas. Si bien estos actores internacionales impulsaron conciencias estatales de seguridad cibernética, no han logrado influir de manera significativa en el proceso securitizador interno, ni en los actores securitizadores, ni en la audiencia.

Las prácticas e instrumentos de securitización en estos dos países responden al desarrollo de los factores internos del discurso securitizador y del contexto histórico. Como se mencionó previamente, las prácticas son consideradas como resultados mediatos del proceso securitizador. Por lo tanto, el mayor alcance del discurso securitizador en Uruguay, un contexto en el que se desarrolla en mayor medida el objeto referente y la aceptación de la audiencia de las medidas extraordinarias, permitieron al Estado ejecutar herramientas de seguridad cibernética. Herramientas que aportan a la construcción de la agenda de seguridad cibernética. Ecuador, por su lado, presenta un menor número de prácticas y menor influencia en la construcción de ciberseguridad dentro del país.

Con relación a las modalidades de securitización, una vez analizados todos los elementos que conforman el proceso securitizador en los dos casos empíricos se puede mencionar que en Ecuador ni Uruguay se ha configurado procesos de hipersecuritización del espacio cibernético. Al contrario, se debería considerar la construcción de una agenda específica de seguridad cibernética que englobe todas las medidas que el Estado debe tomar en pro de la seguridad en este escenario. No obstante, los procesos que han sido analizados podrían enmarcarse en otras modalidades de securitización desarrolladas por Hansen y Nissebaum. Es aquí donde se encuentra una diferencia más que podría ser importante al momento de entender el desarrollo de Uruguay frente a Ecuador en temas de seguridad cibernética.

La forma en la que han actuado los actores securitizadores en Uruguay, así como el contenido de su discurso se ha enfocado en experiencias individuales. La concientización sobre riesgos y amenazas inherentes al uso cotidiano de las tecnologías de la información y la comunicación han buscado la aceptación del individuo. Es decir que, en Uruguay el proceso securitizador del espacio cibernético se desarrolla por medio de la modalidad de prácticas diarias. El proceso en Ecuador, por su lado, se ha enmarcado en la modalidad denominada tecnificación. Si bien esta modalidad no tiene un alto componente político, se considera que el alto componente racional y técnico no permitiría una respuesta mayoritaria de la audiencia.

Finalmente, los actores securitizadores, en los dos casos, han sido primordialmente gubernamentales. Es importante notar que en el caso del discurso para la seguridad cibernética no existe una amplia participación de los presidentes. Si bien estos actores están en una posición de poder frente al resto de instituciones del Estado y cuentan con legitimidad

popular para que la audiencia acepte el discurso de seguridad cibernética, las instituciones gubernamentales de carácter técnico han sido las encargadas del proceso.

Recomendaciones

A manera de recomendación, si bien Uruguay inició un proceso securitizador del espacio cibernético antes que Ecuador, la aceptación de medias extraordinarias como resultado de la intersubjetividad del discurso no responde únicamente a condiciones temporales. Para el desarrollo del proceso securitizador del ciberespacio en Ecuador, se debe fortalecer el discurso, que permita a la audiencia conocer los riesgos y amenazas del objeto referente. A diferencia de Uruguay, Ecuador necesita la participación de ciertos sectores de la sociedad que, además de participar como audiencia, se conviertan en actores securitizadores que permitan desde su posición, motivar la creación de medidas de seguridad por parte del Estado. La política pública podría direccionarse en la concientización de la sociedad sobre el espacio cibernético y en la educación sobre los derechos y garantías que se verían afectados en caso de un ciberataque.

Uno de los actores más importantes es la academia. De ahí nace la necesidad de continuar impulsando estudios que profundicen la temática que ha sido abordada en esta investigación, no únicamente en el aspecto técnico, sino además en las razones sociales, políticas e internacionales que afectan a la implementación de medidas, prácticas o herramientas de seguridad cibernética. Cada factor puede ser analizado en su individualidad, lo cual generaría aportes académicos para el correcto desarrollo de las agendas de seguridad cibernética.

Lista de referencias

AGESIC & INE. 2016. «Encuesta Específica de Acceso y Uso de TIC (EUTIC).» *Uruguay Digital.* https://www.agesic.gub.uy/innovaportal/file/115/2/eutic2016_final.pdf.

AGESIC. 2008. «Agenda Digital Uruguay 2008-2010 para la Sociedad de la Información y el Conocimiento.» 22 de 05. http://uruguaydigital.gub.uy/wps/wcm/connect/urudigital/bf55a088-c5dc-43d6-b932-fdab39fd6e41/ADU+II+2008-2010.pdf?MOD=AJPERES.

—. 2011. «Agenda digital Uruguay 2011-2015: 15 objetivos para el 2015.» *Presidencia de la República Oriental del Uruguay.* https://www.agesic.gub.uy/innovaportal/file/1443/1/agesic_agendadigital_2011_2015.pdf.

—. 2016. «Agenda Uruguay Digital: Transformación con equidad 2020.» *Presidencia de la República Oriental del Uruguay.* https://www.agesic.gub.uy/innovaportal/file/6122/1/agenda-uruguay-digital---enero-final.pdf.

—. 2016. «Encuesta Específica de Acceso y Uso de TIC (EUTIC 2016).» https://www.agesic.gub.uy/innovaportal/file/115/2/eutic2016_final.pdf.

—. 2018. *Estadística de incidentes 2017.* 18 de 01. https://www.cert.uy/inicio/novedades/alertas_y_vulnerabilidades/estadistica+de+incidentes+2017.

—. 2016. *Estadística de incidentes CERTuy 2015.* 09 de 01. https://www.cert.uy/inicio/novedades/alertas_y_vulnerabilidades/estadistica_de_incidentes_certuy_2015.

—. 2017. «Estudio de Conocimientos, Actitudes y Prácticas de Ciudadanía Digital.» *Principales Resultados 2017.* https://www.agesic.gub.uy/innovaportal/file/6888/1/resultados-cap-2017-presentacion-conferencia-4.pdf.

—. 2017. *Iniciativas: Seguridad y confianza.* 09 de 11. https://www.agesic.gub.uy/innovaportal/v/3986/1/agesic/seguridad-y-confianza.html.

—. 2014. *Innovación.* https://www.agesic.gub.uy/innovaportal/v/4099/1/agesic/innovacion.html?idPadre=3930.

—. 2014. *Qué es Agesic.* 04 de 09. https://www.agesic.gub.uy/innovaportal/v/33/1/agesic/que-es-agesic.html.

—. 2007. «Recomendaciones de metas y objetivos para la Agenda Digital Uruguay 2007-2008 para la Sociedad de la Información y el Conocimiento.» *Presidencia de la República Oriental del Uruguay.* http://uruguaydigital.gub.uy/wps/wcm/connect/urudigital/64893207-79f3-4de8-9405-c9727f678d49/ADU+I+2007-2008.pdf?MOD=AJPERES.

—. 2018. *Seguridad y confianza.* 31 de 01. https://www.agesic.gub.uy/innovaportal/v/3986/1/agesic/seguridad-y-confianza.html.

—. 2011. «Sociedad de la Información y Brecha Digital.» *Uruguay Digital.* https://www.agesic.gub.uy/innovaportal/file/20/1/sociedad_de_la_informacion_y_brecha_digital.pdf.

ARCOTEL. 2016. «Hoy empieza evento mundial de ciberseguridad en Quito.» 27 de junio. http://www.arcotel.gob.ec/hoy-empieza-evento-mundial-de-ciberseguridad-en-quito/.

Balzacq, Thierry. 2005. «The Three Faces of Securitization: Political Agency, Audience and Context.» *European Journal of International Relations* 11 (2): 171 - 201. doi:10.1177/1354066105052960.

Balzacq, Thierry. 2011. «Theory of Securitization: Origins, Core Assumptions, and Variants.» En *Securitization Theory: How Security Problems Emerge and Dissolve, ...* Londres: Routledge.

Balzacq, Thierry, Sarah Léonard, y Jan Ruzicka. 2015. «'Securitization' revisited: Theory and cases.» *International Relations* 1-38. doi:10.1177/0047117815596590.

Bendrath, Ralf, Johan Eriksson, y Giampiero Giacomello. 2007. «From “Cyberterrorism” to “Cyberwar,” Back and Forth: How the United States Securitized Cyberspace.» En *International Relations and Security in the Digital Age*, de Johan Eriksson y Giampiero Giacomello, 57 - 82. Londres: Routledge.

Bertón, Juan, Patricia Totorica, y Silvia González. 2013. «Estudio de Conocimientos, Actitudes y Prácticas de Ciudadanía Digital 2013.» *AGESIC.* https://www.agesic.gub.uy/innovaportal/file/3358/1/estudio_conocimiento_actitudes_y_practicas_2013.pdf.

BID y OEA. 2016. *Ciberseguridad ¿Estamos preparados en América Latina y el Caribe?* Informe de Ciberseguridad 2016, Observatorio de la ciberseguridad en América Latina y el Caribe.

Brúculo, Romina, y Alejandro Venczel. 2012. «Defensa cibernética en América del Sur. Estrategias en la UNASUR ante ciberguerra y ciberdelito.» *VI Congreso de Relaciones Internacionales.*

Bull, Hedley. 2002. *The Anarchical Society: a Study of order in World Politics.* New York: Columbia University Press.

Buzan, Barry, Ole Waever, y Jaap de Wilde. 1998. *Security: A New Framework for Analysis.* Cambridge: Lynne Rienner Publishers.

Carlini, Agnese. 2016. «Ciberseguridad: un nuevo desafío para la comunidad internacional.» *Instituto Español de Estudios Estratégicos* (67/2016). http://www.ieee.es/Galerias/fichero/docs_opinion/2016/DIEEEO67-2016_Ciberseguridad_Desafio_ComunidadInt_ACarlini.pdf.

Cavelty, Dunn. 2008. *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age.* Nueva York: Routledge.

CIA. 2018. *The World Factbook.* https://www.cia.gov/library/publications/the-world-factbook/geos/ec.html

CERTuy. 2018. *Institucional.* enero. https://www.cert.uy/inicio/institucional/.

Deibert, Ronald. 2002. «Circuits of Power: Security in the Internet Enviroment.» *Information Technologies and Global Politics. The Changing Scope of Power and Governance.*

Department of State. 2016. «International Cyberspace Policy Strategy.» marzo. https://www.state.gov/documents/organization/255732.pdf.

ecucert. 2017. *Nosotros.* https://www.ecucert.gob.ec/nosotros.html.

El Universo. 2012. «Julian Assange se refugia en embajada de Ecuador en Londres.» 19 de 06. http://www.eluniverso.com/2012/06/19/1/1355/canciller-patino-anuncia-julian-assange-pidio-asilo-ecuador.html.

Erikson, Johan, y Giampiero Giacomello. 2006. «The Information Revolution, Security, and International Relations: (IR) Relevant Theory?» *International Political Science Review* 27 (3): 221 - 244.

Grieco, Joseph. 1988. «Anarchy and the Limits of Cooperation: A Realist Critique of the Newest Liberal Institutionalism.» *International Organization* (MIT Press) 42 (3): 485-507.

Grocio, Hugo. 1925. *De la Guerra y de la Paz.* Madrid: REUS S.A.

Hansen, Lene, y Helen Nissenbaum. 2009. «Digital Disaster, Cyber Security, and the Copenhagen School.» *International Studies Quarterly* (53): 1155-1175.

Hurd, Ian. 2008. «Constructivism.» En *The Oxford Handbook of International Relations*, de Christian Reus-Smit y Duncan Snidal, 298-316. Nueva York: Oxford University Press.

Ibarra, Virginia, y Mónica Nieves. 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* http://sedici.unlp.edu.ar/bitstream/handle/10915/58156/Documento_completo.pdf-PDFA.pdf?sequence=1.

Instituto Nacional de Estadística. 2010. «Principales Resultados Encuesta Usos de las Tecnologías de la Información y Comunicación.» http://www.ine.gub.uy/documents/10181/35933/Principales+Resultados+de+la+Encuesta+de+Usos+de+las+Tecnolog%C3%ADas+de+la+Informaci%C3%B3n+y+las+Comunicaciones+2010/fad55643-d5cb-43db-8a14-14baa808608c.

—. 2013. «Principales Resultados Encuesta Usos de las Tecnologías de la Información y Comunicación.» http://www.ine.gub.uy/documents/10181/35933/Principales+Resultados+de+la+Encuesta+de+Usos+de+las+Tecnolog%C3%ADas+de+la+Informaci%C3%B3n+y+Comunicaciones+2013/504351ca-e277-4efb-82de-f2f70e9a4452.

International Telecommunication Union. 2017. *Global Cybersecurity Index (GCI) 2017.* ITU. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-R1-PDF-E.pdf.

Jaramillo, Paula, y Leandro Ucciferri. 2016. «Vigilancia e inteligencia en la agenda latinoamericana de ciberseguridad. Reporte comparado Chile Argentina.» Cyber Stewards Network. https://derechosdigitales.org/wp-content/uploads/Reporte-comparado-Chile-Argentina.pdf.

Kant, Immanuel. 1795. «Preliminary articles for perpetual peace among states.» https://www.mtholyoke.edu/acad/intrel/kant/kant1.htm.

Karns, Margaret, y Karen Mingst. 2004. *International Organizations: The Politics and Processes of Global Governance.* Colorado: Lynne Rienner Publishers, Inc.

Keohane, Robert. 1986. «Theory of World Politics: Structural Realism and Beyond.» En *Neorrealism and its Critics*, de Robert Keohane Ed. New York: Columbia University Press.

Keohane, Robert, y Joseph Nye. 1988. «Poder e Interdependencia.» *La Política mundial en transición* (Grupo Editor Latinoamericano).

Kremer, Jens. 2014. «Policing cybercrime or militarizing cybersecurity? Security mindsets and the regulation of threats from cyberspace.» *Information & Communications Technology Law* 23 (3): 220-237. doi:10.1080/13600834.2014.970432.

Leiva, Eduardo. 2015. «Estrategias Nacionales de Ciberseguridad: Estudio comparativo basado en enfoque top-down desde una visión global a una visión local.» *Revista Latinoamerica de Ingeniería de Software* 3 (4): 161 - 176.

Lewis, James. 2014. «National Perceptions of Cyber Threat.» *Strategic Analysis* 566 - 576.

Medina, Fernando. 2016. «'Hackers' de Rusia, China, EE.UU y Francia dirigen ataques a Ecuador.» *El Comercio*, 29 de octubre. http://www.elcomercio.com/actualidad/hackers-rusia-ecuador-ciberataques-seguridad.html.

Mill, John Stuart. 2009. *A System of Logic, Ratiocinative and Inductive.* Nueva York: Harper & Brothers, Publishers.

Ministerio del Interior. 2017. *Operación: "Bitcoins".* 12 de 09. https://www.minterior.gub.uy/index.php?option=com_content&view=article&id=4971.

MINTEL. 2018. *Ejes Estratégicos.* https://www.telecomunicaciones.gob.ec/funciones-atribuciones-2/.

—. 2018. *Indicadores y Estadística.* https://observatoriotic.mintel.gob.ec/estadistica/index.html.

—. 2018. *Objetivos.* https://www.telecomunicaciones.gob.ec/objetivos/.

—. 2016. «Plan Nacional de Telecomunicaciones y Tecnologías de Información del Ecuador 2016 - 2021.» https://www.telecomunicaciones.gob.ec/wp-content/uploads/2016/08/Plan-de-Telecomunicaciones-y-TI..pdf.

MINTEL/CDV. 2016. «El MINTEL participó en el 4to. Congreso de Ciberseguridad en Banca y Gobierno.» https://www.telecomunicaciones.gob.ec/mintel-participo-4to-congreso-ciberseguridad-banca-gobierno/.

Morgenthau, Hans. 1986. *Política entre las naciones: La lucha por el poder y la paz.* Buenos Aires: Grupo Editor Latinoamericano.

Noboa, Gustavo. 2000. «Plan de Gobierno 2000 - 2003. Por un nuevo país.» *ODEPLAN.* agosto. http://www.ilo.org/wcmsp5/groups/public/@ed_emp/@emp_policy/@invest/documents/genericdocument/wcms_asist_7639.pdf.

Observatorio de la Ciudadanía. 2014. «Estudio de Conocimientos, Actitudes y Prácticas de Ciudadanía Digital.» *AGESIC.* https://www.agesic.gub.uy/innovaportal/file/3840/1/informe_estudio_cap_v4.0.pdf.

OEA. 2015. «Reporte de Seguridad Cibernética e Infraestructura Crítica de las Américas.» https://www.sites.oas.org/cyber/Documents/2015%20-%20OEA%20Trend%20Micro%20Reporte%20Seguridad%20Cibernetica%20y%20Porteccion%20de%20la%20Inf%20Critica.pdf.

Office of the Coordinator For Cyber Issues. 2015. «International Security.» agosto. https://2009-2017.state.gov/documents/organization/255014.pdf.

ONU. 2010. *Informe del Grupo de Expertos Gubernamentales sobre los avances en la información y las telecomunicaciones en el contexto de la seguridad internacional* . A/65/201. http://www.un.org/es/comun/docs/index.asp?symbol=A/65/201&referer=http://www.un.org/es/ga/.

Orozco, Gabriel. 2006. «El concepto de la seguridad en la Teoría de las Relaciones Internacionales.» *CIDOB d'Afers Internacionals* (72): 161 - 180.

Pardo, Virginia, Federico Monteverde, y Mauro D.Ríos. 2008. «El Gobierno Electrónico en la agenda de la Transformación del Estado.» *Transformación, Estado y Democracia* 3 (37): 31-36. https://www.onsc.gub.uy/onsc1/index.php?option=com_content&view=article&id=198&Itemid=108.

Pereiro Alonso, María Claudia. 2011. «Seguridad de la información en el Uruguay: políticas de Estado en la administración pública.» *Revista de la Asociación de Escribanos del Uruguay* 97: 137-155.

Porcelli, Emanuel. 2013. «Lo esencial es invisible a los ojos. El Constructivismo en las Relaciones Internacionales.» En *Relaciones internacionales: teorias y debates*, de Elsa Llenderrozas. Buenos Aires: Eudeba.

Presidencia de la República de Uruguay. 2000. *Comité Nacional para la Sociedad de la Información.* http://archivo.presidencia.gub.uy/mem2000/info/CNSI.htm.

—. 2015. «Gobierno instauró oficina para fortalecer la seguridad informática de Uruguay.» 30 de 01. http://www.presidencia.gub.uy/comunicacion/comunicacionnoticias/mdn-seguridad.informatica.

Presidencia de la República Oriental del Uruguay. 2014. «2do. Plan de Acción Uruguay 2014-2016.» *Alianza para el Gobierno Abierto.*

https://www.agesic.gub.uy/innovaportal/file/3801/1/plan_accion_uruguay_2014-2016_f.pdf.

—. 2016. «3er Plan de Acción Nacional de Gobierno Abierto de Uruguay.» *Plan de acción de Gobierno Abierto.* https://www.agesic.gub.uy/innovaportal/file/6048/1/3er-plan-de-accion-gobierno-abierto.pdf.

—. 2012. «Plan de Acción Uruguay 2012.» *Sociedad de Gobierno Abierto.* https://www.agesic.gub.uy/innovaportal/file/2062/1/plan_accion_uruguay_2012.pdf.

Quintero, Daniel. 2014. «Las políticas regionales sobre ataques informáticos y su incidencia en la vulnerabilidad de la defensa de la UNASUR en el período 2009 - 2013.» IAEN. http://repositorio.iaen.edu.ec/bitstream/24000/3782/1/TESIS-DANIEL%20QUINTERO.pdf.

Reus-Smit, Christian. 2005. «Constructivism.» En *Theories of International Relations,* de Scott Burchill et. al., 188-212. New York: Palgrave Macmillan.

Rocca, Marco Antonio. 2001. «Las tecnologías de información y comunicación para el desarrollo humano. Informe sobre Desarrollo Humano Ecuador 2001.» *PNUD.* novimebre. http://hdr.undp.org/sites/default/files/ecuador_2001_sp.pdf.

Salter, Mark. 2008. «Securitization and Desecuritization: A Dramaturgical Analysis of the Canadian Air Transport Security Authority.» *Journal of International Relations and Development* 11 (4).

Sanahuja, José, y Julia Schünemann. 2012. «El nexo seguridad-desarrollo: entre la construcción de la paz y la securitización de la ayuda.» En *Construcción de la Paz, Seguridad y Desarrollo. Visiones, Políticas y Actores*, de Sanahuja Jose. Madrid: Complutense S.A.

Secretaría Nacional de la Administración Pública. 2014. «Mensaje del Secretario Nacional de la Administración Pública.» En *Plan Nacional de Gobierno Electrónico 2014 - 2017*, de Vinicio Alvarado, 7.

—. 2014. «Plan Nacional de Gobierno Electrónico 2014 - 2017.» https://ec.network.okfn.org/files/2014/12/PlanGobiernoElectronicoV1.pdf.

U.S. State Department. 2017. *Office of the Coordinator for Cyber Issues.* 20 de enero. https://2009-2017.state.gov/s/cyberissues/.

UN. 2010. «E-Government Survey 2010: Leveraging e-government at a time of financial and economic crisis.» https://publicadministration.un.org/egovkb/Portals/egovkb/Documents/un/2010-Survey/Complete-survey.pdf.

—. 2016. «United Nations E-Government Survey 2016, e-government in support of sustainable development.» http://workspace.unpan.org/sites/Internet/Documents/UNPAN97453.pdf.

URCDP. 2016. *Tus datos valen.* https://www.datospersonales.gub.uy/inicio/sobre+datos+personales/ciudadanos/tusdatosvalen.

Velásquez, Rafael, y Salvador González. 2014. «El realismo clásico.» En *Teorías de las Relaciones Internacionales en el siglo XXI: Interpretaciones críticas desde México*, de Jorge Shiavon et. al., 211-227. Puebla: Universidad Autónoma de Puebla.

Waever, Ole. 1995. «Securitization and Desecuritization.» En *On Security*, de Ronnie Lipschutz, 46 - 87. Columbia University Press.

Waltz, Kenneth. 1988. *Teorúa de la Política Internacional.* Buenos Aires: Grupo Editor Latinoamericano.

Wendt, Alexander. 2004. *Social Theory of International Relations.* Cambridge: Cambridge University Press.

Whetherell, Margaret. 2001. «Debates un Discourse Research.» En *Discourse Theory and Practice: A Reader*, de Margaret Wetherell, Stephanie Taylor y Simeon Yates. Londrés: SAGE.

White House. 2011. «International Strategy for Cyberspace.» mayo. https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.