Las estrategias de ciberseguridad y ciberdefensa en Argentina: marco político-institucional y normativo

1. Introducción

La preocupación por la seguridad de los sistemas de información y comunicaciones viene desde hace años generando políticas, programas y distinto tipos de normas en la República Argentina. El país, si bien no se encuentra entre los blancos principales de las ciberoperaciones, ha sido víctima en una gran cantidad de oportunidades de distintos tipos de ciberataques contra los sitios web de los principales órganos de gobierno (Borghello y Temperini, 2013).

A modo de ejemplo, un incidente de gran relevancia ocurrió en el año 2010 cuando un ciberataque contra el sitio web de la Administración Federal de Ingresos Públicos (AFIP) produjo un fallo en la validación de datos y el acceso a los datos personales de los contribuyentes, tales como copia del DNI, firma y huella digital (Borghello y Temperini, 2013). La mayoría de estos sucesos no cobran notoriedad pública, pues darían cuenta de la existencia de grandes vulnerabilidades en los sistemas y redes gubernamentales; sin embargo, generan la urgencia de mejorar las medidas de seguridad informática a fin de evitar cualquier consecuencia indeseada que estas ciberoperaciones pudieran originar.

Entre tales consecuencias, Borghello y Temperini (2013) destacan el daño a la imagen de la organización gubernamental afectada; el acceso indebido o modificación de datos personales contenidos en bases de datos; la posible afectación de los recursos del usuario y la vulneración del derecho a la protección de los datos personales de los ciudadanos. En tal sentido, cabe destacar que la información que maneja cualquier tipo de organismo, ya sea público o privado, necesita de medidas de seguridad que garantice la protección de la información, lo que implica preservar su confidencialidad, integridad y disponibilidad.

A esta cuestión se suma la importancia de la protección de las denominadas infraestructuras críticas de la información[1], frente a incidentes[2] que pudieran, interrumpir un servicio o el procesamiento de un sistema, pudiendo afectar la provisión de servicios básicos, comunicaciones y el transporte, en tanto los casos más graves podrían llegar a atentar contra la vida misma. Si bien ejemplos de esta gravedad aún no se han conocido (Rid, 2011), muchos Estados han decidido actuar en forma preventiva mediante el desarrollo de estrategias y políticas nacionales destinadas a garantizar la seguridad de las redes y los sistemas de tales infraestructuras estratégicas y vitales.

Para contrarrestar a estos riesgos, la Oficina Nacional de Tecnologías de la Información (ONTI), dependiente de la Jefatura de Gabinete de Ministros se constituye como el organismo responsable a nivel nacional de establecer los lineamientos y programas en materia de seguridad de la información en la Administración Pública Nacional, teniendo por competencias:

- La implementación de estrategias de innovación informática en la administración pública.
- El desarrollo de sistemas informáticos de procedimientos de gestión y el apoyo a organismos públicos para la implementación de portales informativos o de gestión. En este marco, se destaca el Plan Nacional de Gobierno Electrónico.
- El establecimiento de estándares nacionales para la incorporación de nuevas tecnologías de la información.
- La promoción de la interoperabilidad de las redes de información de las instituciones estatales.

[1] Por "infraestructuras críticas de la información" se entiende a aquellas instalaciones, redes, servicios y equipos físicos y tecnologías de la información -hardware y software- de tipo estratégico cuyo funcionamiento es indispensable para brindar servicios a los ciudadanos y las instituciones.

[2] Por incidente nos referimos a todo "evento adverso en un sistema de computadoras, o red de computadoras, que puede comprometer o compromete la confidencialidad, integridad y/o disponibilidad de la información. Puede ser causado mediante la explotación de alguna vulnerabilidad o un intento o amenaza de romper los mecanismos de seguridad existentes" (Disposición ONTI 3/13, Anexo I, pp.16-17).

- La implementación y control del uso de la certificación digital del Estado (firma digital).

- La coordinación en la Administración Pública Nacional de las respuestas ante intentos de ataque o penetración a las redes informáticas de los organismos públicos, fijando parámetros de seguridad y controlando su cumplimiento. Para ello, en el año 2011 la ONTI desarrolló el Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad (ICIC).

2. Política nacional de ciberseguridad

A fines de detallar los antecedentes de la actual política de ciberseguridad, podemos mencionar que en septiembre de 2003, la ONTI[3] inició un trabajo de diagnóstico con especialistas en seguridad informática de diversos organismos públicos dirigido a elaborar una estrategia para el Sector Público Nacional. De ese trabajo surgió la necesidad de elaborar una política nacional y procedimientos de seguridad para la adopción por parte de cada organismo de la Administración Pública Nacional. El primer paso se dio a través de la Decisión Administrativa Nº 669/2004 de la Jefatura de Gabinete de Ministros que estableció la adopción por parte de los organismos del Sector Público Nacional[4] de la "Política de Seguridad Modelo" y la conformación de un Comité de Seguridad de la Información. En el año 2005, a través de la Disposición N° 6/2005 de la ONTI, es aprobada dicha "Política de Seguridad de la Información Modelo".

Dado el incremento en cantidad, variedad y sofisticación de amenazas y vulnerabilidades que pueden afectar los activos de información –como los códigos maliciosos o "DoS", ataques de negación del servicio–, la "Política de Seguridad Modelo" fue ajustada posteriormente a través de la Disposición ONTI 3/2013, en base

[3] A través del Decreto Nº 1028/03 se le otorgó a la ONTI la responsabilidad de entender, asistir y supervisar os aspectos relativos a la seguridad y privacidad de la información digital y electrónica del Sector Público Nacional.

[4] Alcanza a la Administración Central y los Organismos Descentralizados, comprendiendo a las Instituciones de Seguridad Social y a aquellos Entes Públicos excluidos expresamente de la Administración Nacional, de acuerdo al art. 8 de la Ley Nº 24.156.

a las actualizaciones sufridas por la norma ISO/IEC 27.002, a fin de mantener su vigencia y nivel de eficacia.

Paralelamente, en julio de 2011, Argentina lanzó el Programa Nacional de Infraestructuras Criticas de Información y Ciberseguridad (ICIC)[5], con el propósito principal de desarrollar las políticas y regulaciones asociadas a la protección de las infraestructuras estratégicas de la información del Estado[6].

Según el Director del programa, Pedro Janices, el ICIC surgió "de la necesidad que todo gobierno tiene de reaccionar ante situaciones críticas que afecten el normal desenvolvimiento de aquellos sistemas que sean fundamentales para el accionar diario de los ciudadanos. Dentro de ellos, las redes de comunicación informática y sus datos, cumplen un rol esencial en la actualidad. Yendo específicamente a lo digital, cumple las tareas de relevar y prevenir todos aquellos actos que intenten vulnerar los sistemas del Estado o a sus ciudadanos" (Holloway, 2001).

Para llevar adelante este proceso, el ICIC conformó cuatro grupos de trabajo:

- El Equipo de Respuesta ante Emergencias Teleinformáticas (CERT), que brinda asistencia y asesoramiento en el análisis de los incidentes y formula recomendaciones para su tratamiento.
- El Grupo de Acción Preventiva (GAP), responsable del estudio de posibles fallas de seguridad y las acciones preventivas que posibiliten la reducción de incidentes de seguridad informática. También tiene como misión elaborar las "Políticas de Seguridad", basadas en las normas internacionales ISO 27.001 y 27.002, así como dar asesoramiento para su implementación.
- El grupo INTERNET SANO, que consiste en un programa educativo que posee por objeto brindar concientización y capacitación en materia de ciberseguridad, especialmente entre niños y jóvenes.

[5] Resolución Nº 580/2011.

[6] Cabe señalar que pueden participar del programa organizaciones civiles y también aquellos organismos del sector privado que soliciten su adhesión

- El Grupo de Infraestructuras Críticas de la Información (GICI), responsable del relevamiento, identificación y clasificación de las infraestructuras estratégicas y criticas de información, del monitoreo de los servicios que el Sector Público Nacional brinda a través de Internet, de la coordinación de los ejercicios de respuesta ante un intento de vulneración de tales infraestructuras críticas, así como también de brindar asesoramiento sobre tecnologías de la información y propiciar la articulación con el sector privado.

Complementariamente, el ICIC posee el apoyo de un grupo de especialistas en temas jurídicos, para la asistencia en todos aquellos aspectos vinculados al marco normativo en materia de ciberseguridad.

Finalmente, resta mencionar que los esfuerzos realizados al momento y a partir de la amplia participación de los distintos sectores del ámbito público, se está avanzando en la elaboración de una Estrategia Nacional de Ciberseguridad.

Legislación nacional

En referencia a la legislación nacional, y tal como se ha dicho precedentemente, los intentos por parte de los distintos niveles gubernamentales con el objetivo de regular el uso que hacen los ciudadanos del ciberespacio son cada vez más frecuentes y masivos a partir de la creciente importancia que ha tenido Internet en estos últimos años.

Por otra parte, se puede agregar que los cambios de una sociedad, y los procesos sociales que estos acarrean al interior de ella generan, análogamente, acciones por parte de distintas instituciones que giran en torno a esas cuestiones o temas que se originan, adquiriendo significación sólo en el caso de que sean vinculadas a ellos (O´Donnell *et al*, 1982). Así, a medida que haya necesidades y demandas en las continuas y dinámicas interacciones internas de la sociedad, alguna de ellas será problematizada, incorporándose a la “agenda de problemas socialmente vigentes”

(O´Donnell *et al*: 109) ante la cual el Estado y sus representantes tendrán que adoptar una posición frente a cada uno de los temas postulados. Si bien este tipo de proceso se utiliza para llegar a una explicación sobre la hechura de las políticas públicas, podría extrapolarse a la sanción y promulgación de leyes en el territorio nacional, en tanto se conforman en el marco jurídico en el que deben insertarse dichas políticas.

En este sentido, la República Argentina, a partir del auge de Internet y de los continuos casos de intrusión en las redes, ya sean identificados como ciberataques de distintos Instrumentos Militares o como delitos provenientes de los llamados hackers, ha comenzado a tomar las medidas necesarias para proteger a los ciudadanos y a los diversos organismos públicos de este tipo de actividades.

En primer lugar, la Ley 25.326 de Protección de Datos Personales es la ley marco que regula la protección de los datos personales en nuestro país, y que busca garantizar el derecho al honor, a la privacidad y a la intimidad de la personas, y el acceso a la información que pueda registrarse sobre estas. Este marco regulatorio se “opone” a las normas sobre acceso a la información pública que existen en cada una de las jurisdicciones (el Decreto 1.172/2003 en el ámbito federal). Paralelamente, establece los derechos de los titulares de los datos, las responsabilidades ligadas a los archivos y bancos de datos, los mecanismos de control, las sanciones y los procedimientos pertinentes. Pero también obliga a los responsables o usuarios de datos a adoptar las medidas técnicas y organizativas necesarias para garantizar la seguridad y confidencialidad de los datos personales; y prohíbe el registro de datos personales en archivos, registros o bancos que no reúnan las condiciones técnicas de integridad y seguridad necesarias (Art. 9). También prohíbe la transferencia de datos personales a países u organismos internacionales que no proporcionen niveles de protección adecuados y sus respectivas excepciones (Art. 12). Por otro lado, el artículo 21 obliga a los bancos de datos (públicos y privados) a estar registrados y a informar los medios utilizados para garantizar la seguridad de los datos. Debe destacarse que también están sujetos a esta ley, los datos personales que por haberse almacenado para fines administrativos, deban ser objeto de registro permanente en los archivos de las Fuerzas Armadas (Art. 23).

Esta Ley fue reglamentada por el Decreto Nº 1.558/2001, que a su vez fue modificado por el Decreto Nº 1.160/2010, sin introducirse modificaciones sustanciales a los artículos referenciados.

En el 2008, con el propósito de velar por el derecho a la protección de los datos personales y penalizar las violaciones al "secreto" y a la "intimidad", se dicta la Ley 26.388, de Reforma del Código Penal, reconociéndose de este modo a éstos como bienes jurídicos protegidos. En resumidas cuentas, con esta reforma se incorporan al Código Penal la figura de los delitos informáticos

Otra norma que ya hemos mencionado pero que debemos destacar por la trascendencia que posee en la materia, es la Resolución 580/2011 de la Jefatura De Gabinete de Ministros aprueba el Programa Nacional de Infraestructuras Críticas de Información y de Ciberseguridad, el cual tiene cómo objetivo la elaboración de un marco regulatorio específico que propicie la identificación y protección de las infraestructuras estratégicas y críticas de las entidades y jurisdicciones pertenecientes al Sector Público Nacional, los organismos interjurisdiccionales, y las organizaciones civiles y del sector privado que lo requieran, así como al fomento de la cooperación y colaboración de los mencionados sectores (Articulo 2). El Artículo 3º establece los objetivos específicos del programa.

En cuarto lugar, la Dirección Nacional de Tecnologías de la Información aprobó el formulario de adhesión al "Programa de Nacional de Infraestructuras Críticas de Información y Ciberseguridad" y el texto modelo del "Convenio de Confidencialidad", mediante la Disposición ONTI Nº 3/2011.

Otras normas importantes, aunque no estén destinadas a regular sobre la materia, pero que de algún modo se encuentran vinculadas, son la ley 25.506 sobre firma digital, el Decreto Nº 1.766/2011 que crea el Sistema Federal de Identificación Biométrica para la Seguridad, mediante el cual se genera una inmensa base de datos sobre las personas, y por último, la Ley Nº 25.873, relacionada con la responsabilidad de los prestadores respecto de la captación y derivación de comunicaciones para su observación remota por parte del Poder Judicial o Ministerio Público. Esta norma es

importante porque fue contestada por inconstitucional (junto a su Decreto reglamentario Nº 1.563/2004) y la Corte le dio la razón al demandante. Por ende estableció límites a la intervención de las comunicaciones telefónicas y por Internet, protegiendo la privacidad de los ciudadanos frente a intervenciones del Estado.

Por su parte, el Honorable Senado de la Nación ha recibido varios proyectos de ley por parte de los representantes de los diversos bloques partidarios que lo componen. Del relevamiento realizado, encontramos cinco proyectos de ley y un proyecto de resolución en estado parlamentario, y todos ellos, a pesar de que presentan ciertas diferencias, se vinculan con la llamada "neutralidad en la red".

En orden de comprender mejor lo que abarcan estos documentos parlamentarios, se indica que la neutralidad en la red es un principio que garantiza la igualdad de acceso a contenido, es decir, se basa en la idea de que los proveedores del servicio de Internet otorguen acceso a los contenidos sin que haya de por medio privilegios a un participante de la red por encima de otros. Así, trata como iguales a todos los usuarios conectados con respecto a los paquetes que transporta.

Cabe destacar que los objetivos expresados en cada uno de los proyectos de Ley desarrollados, a pesar de algunas disimilitudes en expresión y vocabulario, se centran en prohibir o restringir a las empresas proveedoras de acceso a Internet de acciones como bloquear, ralentizar, interferir, entorpecer, distinguir, degradar u obstaculizar el derecho con el que cuenta cada uno de los usuarios del servicio o de ciertas aplicaciones para utilizar, enviar, recibir u ofrecer contenido, información o servicio legal a través de Internet. A continuación se realizará un pequeño resumen de los proyectos de ley y del proyecto de resolución que se encuentran en estado parlamentario.

Proyecto de Ley S- 1856/2013

En sus fundamentos, el proyecto de ley señala que el principio de neutralidad en la red está relacionado con el tráfico de datos en internet, indicando que el mismo no debe

ser excluyente, y con el hecho de que los proveedores del servicio no deben dar prioridad a determinados sitios.

A partir de esta aclaración, afirma que el objeto de esta propuesta de ley es que "los usuarios de internet tengan acceso al contenido en la Web sin tener que pasar por la intermediación de los operadores o proveedores del servicio". De esta manera, en uno de los artículos del proyecto de ley se plantea la necesidad de que los proveedores preserven la privacidad, protección y libertad de los usuarios de utilizar instrumentos, aparatos, dispositivos u otros elementos legales para acceder a la red".

Proyecto de Ley S- 2222/13

El propósito de la ley es establecer la neutralidad en la red, con el fin de asegurar a los usuarios de internet el derecho a utilizar, enviar y recibir u ofrecer cualquier contenido, aplicación o servicio a través de internet. Mientras tanto, los proveedores del servicio tendrán prohibido "bloquear, interferir, ralentizar y restringir el derecho de los usuarios de Internet para utilizar". Tampoco podrán enviar, recibir u ofrecer contenidos, fraccionar el cobro del servicio por acceder a determinado tipo de contenido ni limitar el derecho de un usuario a utilizar cualquier hardware o software para acceder al servicio". De lo contrario las empresas sufrirán sanciones que pueden llegar a ser apercibimientos, multas o, directamente, la caducidad de la licencia. La autoridad de aplicación será establecida por el Poder Ejecutivo Nacional.

En cuanto a los fundamentos que otorga el proyecto de ley, indica, dada la gradual importancia de Internet que cala en el interior de la sociedad, es el Estado el responsable de garantizar el acceso a las nuevas tecnologías y de facilitar su utilización por parte de los ciudadanos, avalando el derecho a la comunicación y estableciendo las condiciones necesarias para que ese derecho esté protegido.

Proyecto de Ley S- 2291/2013

Este proyecto de ley busca garantizar una red abierta e ilimitada porque Internet, originalmente, tiene carácter neutral, lo que pretende generar igualdad de condiciones. A fin de lograr esa garantía dentro del territorio nacional, la autoridad de aplicación, en este caso la Secretaría de Comunicaciones de la Nación será la encargada de atender las consultas, las mediciones correspondientes y los procederes de los proveedores de servicio de Internet que resulten incompatibles con el objetivo de la propuesta.

Será de aplicación la Ley 24.240 de "Defensa del Consumidor" en los casos de violación, restricción, menoscabo o cualquier otro caso que impida el cumplimiento de los derechos establecidos en la misma.

Proyecto de Ley S- 3761/2013

Esta propuesta de ley presenta como objetivo "garantizar la neutralidad en la red, de forma tal que cualquier dispositivo conectado a internet pueda comunicarse con otro equipo de la red, sin importar su ubicación, e intercambiar libremente cualquier tipo de dato en condiciones de igualdad, sin tener en cuenta su origen, destino, contenido y/o servicios".

Como autoridad de aplicación de la ley, se postula la Creación de un Consejo Federal de Neutralidad en la Red (CONFER), el cual dictará su propio reglamento y establecerá un régimen sancionatorio para las infracciones contra lo dispuesto en la presente ley y en su reglamentación.

Proyecto de Ley S- 2159/2014

El mismo refiere que, ante un escenario global donde el uso de Internet evolucionó con un significativo impacto positivo, se encuentra conveniente incluir la neutralidad de red como garantía de protección a los usuarios, frente a las nuevas amenazas que acechan. Si bien puede observarse que el carácter original de Internet es evitar todo

tipo de inclusión gubernamental en el régimen ciberespacial, la naturaleza abierta no se encuentra en absoluto garantizada, puesto que los proveedores de acceso a Internet no están dispuestos a propiciar la existencia de una plataforma abierta a contenidos y aplicaciones. Asimismo, esta propuesta acude, dentro del contexto nacional, a que se carece de un marco legal actualizado que regule las comunicaciones, pudiendo sólo recurrir a la Ley Nº 19.798[7], que puesto que es del año 1972, no comprende este nuevo tipo de amenazas a las garantías constitucionales surgidas de la evolución tecnológica de la última década. En este sentido, buscando los mismos objetivos que los proyectos de ley ya mencionados, los proveedores de Internet serán sancionados con apercibimientos, multas y caducidad de la licencia y se graduarán en atención "a la gravedad y reiteración de la infracción, las dificultades o perjuicios que la infracción ocasiones al servicio prestado, a los usuarios y a terceros, al grado de afectación del interés público y al valor de la infraestructura empleada en la comisión de la infracción evaluada" y la autoridad de aplicación será la Comisión Nacional de Comunicaciones.

Con respecto a estos proyectos de ley, el Senado de la Nación comenzó a instalar el debate sobre la llamada "neutralidad en la red". Al no contar ninguno de ellos con diferencias importantes, los senadores de las diversas bancadas, llegaron al acuerdo de unificar todos ellos que derive en una ley consensuada por todos.

Por su parte, el proyecto de Resolución S- 2435/2014 presentando en el Senado de la Nación establece que sería pertinente la inclusión del Honorable Senado de la Nación al Programa Nacional de Infraestructuras Críticas de Información y Seguridad, llevado a cabo por la Oficina Nacional de Tecnologías de la Información, debido a la información sensible que se maneja dentro de él.

[7] Ley Nacional de Telecomunicaciones.

Política de ciberdefensa

En el ámbito del Ministerio de Defensa, el advenimiento de la cada vez más creciente relevancia y complejidad del tema ciberespacial se refleja también en el compendio de resoluciones que fueron firmadas en los últimos tiempos por el titular de la cartera.

La primera de ellas fue la Resolución del Ministerio de de Defensa N° 364 del año 2006 que establece la creación del Comité de Seguridad de la Información en el ámbito del Ministerio de Defensa, el cual está integrado por los Directores Generales de las distintas agencias pertenecientes a la jurisdicción y es coordinado por la Subsecretaría de Coordinación. El origen del mismo se da a partir de la ya mencionada Decisión administrativa N° 669/2004.

En segundo lugar, la Resolución del Secretario de Estrategia y Asuntos Militares N° 08 del año 2010, mediante la cual se creó en el ámbito de esa Secretaria un grupo de trabajo con el fin de analizar y evaluar la relevancia y la implicancia del ciberespacio en la agenda del Sistema de Defensa Nacional.

Por su parte, la Resolución 385/2013, también de la jurisdicción Defensa, conforma, en el ámbito de la Jefatura de Gabinete de Asesores del Ministerio de Defensa, la "Unidad de Coordinación de Ciberdefensa" y establece las funciones e integración de dicha unidad, reuniendo en una sola agencia la coordinación de la política relativa a ciberdefensa en el ámbito de la jurisdicción, con el propósito de "generar mecanismos integrados de respuesta para la toma de decisiones".

De esta manera, las responsabilidades de la unidad serán: coordinar políticas y el desempeño de los actores vinculados a la ciberdefensa, lo que incluye a empresas y organismos descentralizados en su órbita; efectuar y mantener actualizado un relevamiento exhaustivo de infraestructuras, redes, recursos humanos, procesos y actividades relativos a la ciberdefensa en la jurisdicción; entender en el diseño, planificación estratégica e implementación de las políticas de la jurisdicción, impulsar el desarrollo doctrinario en la materia; analizar de modo permanente la evolución normativa en la materia, así como su relación con el marco legal de la defensa; intervenir por la jurisdicción en la implementación de la Resolución JGM N° 580/2011;

desarrollar vínculos de intercambio y cooperación con el ámbito académico y científico; fomentar políticas de convocatoria y formación de recursos humanos específicos; promover la adopción de procedimientos y protocolos comunes.

A partir de la aprobación de la Resolución MD Nº 343/2014, el Instrumento Militar del Sistema de Defensa Nacional comienza a ser incluido en el armado de una estrategia ciberdefensiva. Con ella se crea el Comando Conjunto de Ciberdefensa, dependiente del Estado Mayor Conjunto de las Fuerzas Armadas. Dicha Resolución establece como misión de éste ejercer la conducción de las operaciones de ciberdefensa en forma permanente a los efectos de garantizar las operaciones militares del Instrumento Militar de la Defensa Nacional.

Finalmente, no debe olvidarse que estas medidas son acompañadas también por el compromiso de la República Argentina por articular políticas de defensa cibernética con otros países del ámbito de la UNASUR. Tales acciones confluyen positivamente en el objetivo de la política de defensa argentina de avanzar progresivamente hacia el logro de un sistema de defensa subregional[8]. Efectivamente, el 13 de septiembre de 2013 se suscribió la Declaración de Buenos Aires, una declaración conjunta entre el Ministro de Defensa argentino, Agustín Rossi, y su homólogo del Brasil, Celso Amorim, a través de la cual decidieron impulsar la cooperación en ciberdefensa y la creación de un grupo de trabajo bilateral, el cual se reunió dos meses después en Brasilia y acordó una agenda de trabajo, orientada a las áreas de capacitación, métodos y sistemas tecnológicos, desarrollo de doctrina combinada, investigación científica e intercambios entre los CSIRT –*computer security incident response team*– de ambos Ministerios para incrementar la seguridad cibernética.

[8] Decreto Nº 1714/09, Directiva de Política de Defensa Nacional.

Conclusiones

Como se desarrolló anteriormente, en los últimos años, se han hecho numerosos esfuerzos para comenzar a fortalecer al país en materia de seguridad de la información y ciberdefensa, desde la aparición de ciertos inconvenientes a nivel internacional y doméstico. Sin embargo, es necesario continuar con este proceso, e incluir al mismo, definiciones de tipo académico, de manera de poder dar un final a los debates y discusiones en torno a lo que es la ciberseguridad y ciberdefensa. De tal modo, se observa de relevancia que la futura Estrategia Nacional de Ciberseguridad vincule pluralmente las demandas de los sectores gubernamentales, los poderes legislativo y judicial, con las demandas del sector privado y de las universidades, así como también de organizaciones no gubernamentales.

Si bien, efectivamente, se detecta un marco normativo ya existente que hace referencia a la protección de datos y a la seguridad de la infraestructura crítica de la información, que es la máxima preocupación de la mayoría de los países, queda un largo camino por recorrer alrededor de esta misma temática, y en particular a lo que se considerará como ciberdefensa, y todos los fenómenos que esta distinción acarrea con ella.

En tal sentido, se observa como un desafío importante preservar las infraestructuras críticas de la información, garantizar a nivel del Sistema de Defensa Nacional argentino los sistemas de C3IGE (comando, control, comunicaciones, informática y guerra electrónica) de las Fuerzas Armadas, de cualquier incidente cibernético que pudiera afectar el desarrollo de las operaciones militares, y articular el campo de la ciberdefensa con la política nacional de ciberseguridad, teniendo en cuenta que los sistemas informáticos y de comunicación militares deberían ser considerados como una “infraestructura crítica”, que posee la particularidad de que los mismos deben estar siempre operables y la información contenida o trasmitida a través de ellos segura, para garantizar eficazmente la defensa de la Nación Argentina y la defensa de

nuestros intereses vitales, ante cualquier agresión estatal militar externa. Esta necesidad no quita, sino que conlleva, la necesidad de concertar políticas o mecanismos de ciberdefensa con los países de la región, a fin de preservar a Sudamérica como zona de paz, incluso en el espacio cibernético.

Bibliografía

Bañón, R., Carrillo, E. (1997). *La nueva administración*. Madrid: Edit, Alianza Universidad.

Borghello, C. y Temperini, M. (2013). Seguridad o inseguridad informática. Ciberseguridad Nacional Argentina: Cracking de Servidores de la Administración Pública, en *42 JAIIO Simposio Argentino de Informática y Derecho*, Universidad Nacional de Córdoba. Disponible en http://www.asegurarte.com.ar/material/JAIIO_Temperini_Borghello_Cracking_Servidores.pdf.

Holloway, Christopher (2001). *El Plan Argentino para su ciberseguridad*. Disponible en http://tecno.americaeconomia.com/noticias/el-plan-argentino-para-su-ciberseguridad

Nemirovsci, Martiniano (2014, 21 de septiembre). "Neutralidad en la red: ¿de qué estamos hablando?". *Diario Digital Telám*. Disponible en http://www.telam.com.ar/notas/201409/78963-neutralidad-en-la-red-proyecto-ley-senado.html.

O´Donnell G., Oszlak, O. (1982). Estado y políticas estatales en América Latina: hacia una estrategia de investigación, en *Revista Venezolana de Desarrollo Administrativo*, *1*, pp. 91-135.

Rid, Thomas Rid (2012). Cyber War Will Not Take Place, en *Journal of Strategic Studies*, *35* (1), pp. 5-32.

Documentos oficiales y normativos

Política de Seguridad de la Información Modelo, Anexo I, Disposición ONTI 3/13.

Resolución Nº JGM 580/2011

Ley Nº 24.156

Ley Nº 25.326

Ley Nº 25.506

Ley Nº 25.873

Ley Nº 26.388

Decreto Nº 1028/2003

Decreto Nº 1729/2009

Decreto Nº 1.766/2011

Resolución JGM 580/2011

Resolución MD N° 364/2006

Resolución MD Nº 385/2013

Resolución MD Nº 343/2014

Decisión Administrativa JGM Nº 669/04

Resolución SEAM N° 08 del año 2010

Disposición ONTI N° 6/2005

Disposición ONTI Nº 3/2013

Declaración Conjunta de los Ministros de Defensa de la república Federativa del Brasil y de la República Argentina, Brasilia, 21 de noviembre de 2013.

Declaración de Buenos Aires de los Ministros de Defensa del Brasil y Argentina, Buenos Aires, 13 de septiembre de 2013.

Acta de Reunión del Subgrupo de Trabajo Bilateral de Defensa Cibernética Brasil-Argentina, 20 y 21 de noviembre de 2013.

Proyecto de Ley S- 1856/2013

Proyecto de Ley S- 2222/13

Proyecto de Ley S- 3761/2013

Proyecto de Ley S- 2159/2014

Proyecto de Ley S- 2291/2013

Resolución S- 2435/2014