CIBERSEGURIDAD EN LA ERA DE LA VIGILANCIA MASIVA

Descubriendo la agenda de ciberseguridad de América Latina: El caso de Argentina

por los Derechos Civiles

Área de Privacidad

Mayo 2016

https://adcdigital.org.ar

Índice

I El proyecto **5**

II Ciberseguridad: una primera aproximación **7**

i Factores que inciden en su desarrollo 8

a Del almacenamiento a bajo costo, al lema "recolectarlo todo" 8

b Fácil adquisición de herramientas de vigilancia masiva 9

III Definiendo la ciberseguridad **11**

i (Des)militarizando concepciones: alineando la ciberseguridad con los derechos humanos 14

IV Tendencias internacionales en el desarrollo de políticas de ciberseguridad y su adecuación al contexto latinoamericano **16**

i Una nueva generación de estrategias nacionales de ciberseguridad para la economía de Internet 17

ii Colombia: pionera en América Latina 22

iii La ciberseguridad en el contexto lationamericano desde la OEA . . 26

V En busca de una agenda de ciberseguridad en Argentina **29**

i Coordinación de Emergencia en Redes Teleinformáticas de la Administración Pública Argentina (ArCERT) 30

ii Programa de Infraestructuras Críticas de Información y Ciberseguridad (ICIC) 31

iii Subsecretaría de la Protección de Infraestructuras Críticas de Información y Ciberseguridad 34

iv Nueva Doctrina de Inteligencia Nacional y la Dirección Operacional de Inteligencia sobre la Ciberseguridad 36

v Subsecretaría de Tecnología y Ciberseguridad 39

vi Subsecretaría de Ciberdefensa 41

vii De la normativa a la práctica: el estado de situación real de la ciberseguridad en la Argentina 42

viii Una mirada exterior a la ciberseguridad en la Argentina, con la que no estamos necesariamente de acuerdo 46
a "Seguridad Cibernética e Infraestructura Crítica en las Américas" 46
b "Ciberseguridad: ¿Estamos preparados en América Latina y el Caribe?" 47

VI Inteligencia y ciberseguridad **49**
i El vínculo de la inteligencia con la ciberseguridad 49
ii Breve historia de la inteligencia en democracia, un sistema al que le cuesta abandonar sus vicios 52
iii La Agencia Federal de Inteligencia 54

VII Comentarios finales **56**

VIII Conclusiones **57**

Ciberseguridad en la era de la vigilancia masiva

Descubriendo la agenda de ciberseguridad de América Latina:

El caso de Argentina*

I El proyecto

Las discusiones acerca de la ciberseguridad se están desarrollando en contextos internacionales como el de la Organización de los Estados Americanos (OEA) y sus programas, sin participación de la sociedad civil y sin considerar la perspectiva de protección de los derechos humanos. Por su parte, estas discusiones también tienen lugar en las agendas nacionales, con temas tales como la seguridad del Estado, los mecanismos de inteligencia y las prácticas de vigilancia.

Los trabajos de investigación que han ido desarrollando ADC, Derechos Digitales y otras organizaciones civiles de la región sobre el tema, nos permite describir el siguiente escenario: las prácticas de vigilancia en el Cono Sur, especialmente aquellas ligadas a actividades de inteligencia, no están alineadas con una perspectiva amplia de derechos humanos, no tienen adecuado control y son usualmente fuente de conductas ilegales que terminan violentando derechos de los ciudadanos o debilitando el sistema democrático y sus instituciones. Esto es así pues hay países de Latinoamérica que cuentan con marcos legales que les permiten obtener información de sus ciudadanos en forma masiva y lo que es más grave, los organismos encargados de la recolección de esta información, de la interceptación

*Este informe fue elaborado por Leandro Ucciferri, abogado e investigador de las Áreas de Privacidad y de Libertad de Expresión de la ADC, junto con la colaboración de Valeria Milanes, Directora de las Áreas.

de las comunicaciones, de las tareas de vigilancia y ciberseguridad son usualmente heredadas de gobiernos dictatoriales. Esta herencia por lo general implica métodos opacos, recolección desproporcionada de información, secreto excesivo, falta de transparencia y una larga experiencia en violaciones a derechos humanos que han quedado impunes.

A lo largo de esta investigación publicamos una serie de briefing papers enfocados en explorar distintos aspectos de la ciberseguridad, con el fin último de determinar la existencia y contenido de la agenda de ciberseguridad en Latinoamérica, con especial foco en el caso argentino, para determinar luego su correspondencia con estándares protectorios de derechos humanos y en su caso, efectuar las sugerencias o recomendaciones pertinentes.[1]

En este documento profundizaremos los resultados derivados de los distintos informes, así como también precisaremos sobre el vínculo de la ciberseguridad con el sistema de inteligencia y la vigilancia, que en los últimos años se ha expandido por América Latina.

En el **segundo capítulo** plantearemos la problemática con la cual nos topamos al momento de comenzar a estudiar y analizar el campo de la ciberseguridad, estableciendo el enfoque de la investigación y analizando dos factores que incidieron en el desarrollo de las políticas de ciberseguridad a nivel global. En el **tercer capítulo** exploraremos qué es la ciberseguridad a través de distintos conceptos brindados por diferentes actores globales, sus alcances e implicancias. En el **cuarto capítulo** analizaremos distintos documentos que ponen énfasis en el desarrollo de políticas de ciberseguridad, así como el estado de la ciberseguridad, a nivel global. En el **quinto capítulo** desarrollaremos la evolución normativa de la ciberseguridad en Argentina, analizando en qué ámbitos se encuentra inserto el término, qué uso se hace del mismo y cuáles son los alcances de las normativas. En el **sexto capítulo** analizaremos el vínculo del sistema de inteligencia con la ciberseguridad. Y concluiremos finalmente con nuestros comentarios, reflexiones y recomendaciones sobre el enfoque de la ciberseguridad desde una perspectiva de la sociedad civil y de derechos humanos.

[1] Los briefing papers pueden ser consultados en el sitio web de las áreas de Privacidad y Libertad de Expresión de la ADC: https://adcdigital.org.ar/publicaciones

II Ciberseguridad: una primera aproximación

Antes de poder desarrollar el panorama actual de la ciberseguridad en Argentina, es fundamental tener en claro qué es la ciberseguridad en sí.

Por este motivo encaramos la búsqueda de una definición, en el entendimiento de que encontrarla nos daría el marco dentro del cual se desenvuelve la temática y nos facilitaría la interpretación –más restrictiva o más laxa– de sus alcances y de los diversos elementos que deben tenerse en cuenta al hablar de ciberseguridad.

Sin embargo no fue tan sencillo como podría parecer. En nuestro país no hay todavía una definición consensuada o adoptada unánimemente por los organismos estatales.

De tal suerte, cambiamos el enfoque y buscamos una definición de ciberseguridad en otros entornos nacionales e internacionales.

Pudimos advertir que si bien los intentos por acordar internacionalmente cuestiones relacionadas con Internet y la tecnología no son nuevos, con el debate de la ciberseguridad algunos problemas parecen haberse acentuado. Ello es así ya que los Estados tienen intereses distintos, ya sea sobre cómo debe regularse una actividad, sobre cuál debería ser su conceptualización y alcances, y sobre qué actividades podrían constituir delitos. Es por esto que llegar a un acuerdo sobre una definición resulta una tarea compleja, en la cual se deben considerar múltiples factores. El concepto de ciberseguridad parece estar en pleno desarrollo y una definición precisa ocultaría el hecho significativo de que el concepto, en sí, es objeto de disputas entre distintas miradas, perspectivas e intereses.

Por ello comenzamos a analizar algunos de estos factores y comparamos conceptos utilizados por varios países y por organismos internacionales, en el afán de establecer pautas de análisis que nos permitan comenzar a abordar y entender la agenda de ciberseguridad argentina, para luego establecer su adecuación con estándares protectorios de derechos humanos.

i Factores que inciden en su desarrollo

Como analizaremos con posterioridad a lo largo de este informe, las tendencias recabadas en estudios internacionales y la opinión de los expertos gira en torno al tratamiento de la ciberseguridad como una práctica necesariamente interdisciplinaria, la cual abarca múltiples aspectos de la sociedad y la economía que no solo tienen que ver con una mirada de defensa o militar y de inteligencia. Aún así, múltiples países han iniciado sus procesos de desarrollo de políticas de ciberseguridad con un fuerte vínculo desde la ciberdefensa, la inteligencia y la vigilancia.

En tal sentido, identificamos dos factores que entendemos se han vuelto troncales para comprender el contexto de la elaboración de políticas de ciberseguridad y los discursos que adoptan ciertos países al respecto de esta temática.

a Del almacenamiento a bajo costo, al lema "recolectarlo todo"

La tecnología en el campo del almacenamiento de datos ha dado en los últimos años pasos de gigante en su carrera por abaratar el costo de producción y del producto final. Así, a finales del año 2000, el costo promedio de 1 Gigabyte en almacenamiento era de 10 U$D; para el año 2005, el promedio había bajado a 1 U$D. Diez años después, a finales de 2015, el promedio por GB es de menos de 5 centavos de dólar.

Las empresas y también los gobiernos comenzaron a darse cuenta que no era necesario deshacerse de toda la información que recolectaban de sus usuarios, con la excusa de nunca saber cuándo la necesitarían en el futuro, y sobre todo porque ya no tenían que lidiar con altos costos de almacenamiento. Las bases de datos se fueron convirtiendo poco a poco en co-protagonistas de la economía mundial, del desarrollo de Internet y de la vigilancia estatal y corporativa.

En tal sentido, los Estados también se vieron involucrados en este cambio de paradigma del almacenamiento de información, aún mediante el uso de prácticas que pueden ser consideradas netamente ilegales.

El caso más emblemático, y que se perfila como el más importante de la década, fue aquel denunciado por Edward Snowden (ex-analista de la NSA) en el año 2013, quien filtró miles de documentos que ponen de manifiesto los programas llevados a cabo por la Agencia Nacional de Seguridad (National Security Agency) de Estados Unidos y de la Oficina Central de Comunicaciones Gubernamentales (Government Communications Headquarters) que tienen como actividad primordial el almacenamiento masivo e indiscriminado de información, todos con plazos distintos. Por ejemplo, 3 días para el contenido de llamadas y emails bajo el programa XKEYSCORE; 1 año para el historial de navegación bajo el programa MARINA; y 5 años para los metadatos de llamadas telefónicas; todo esto sin olvidar que cuando un analista utiliza de alguna manera datos almacenados, su plazo de retención pasa a ser ilimitado. Este es el reflejo del lema de la NSA, "Recolectarlo todo. Saberlo todo", hacer una copia lo más detallada posible sobre la vida digital de la mayor cantidad de personas posibles alrededor del mundo, tan solo por si algún día resulta necesario utilizarlo cuando esas personas se conviertan en un objetivo o enemigo.

b Fácil adquisición de herramientas de vigilancia masiva

Sumado al factor sobre el almacenamiento de datos de los ciudadanos, encontramos a su vez que las herramientas de vigilancia masiva son cada vez más fáciles de adquirir, pues su desarrollo ha dejado de ser de exclusivo monopolio militar o estatal. El caso más reciente es el de la empresa italiana Hacking Team, conocida por vender software espía y utilidades para el acceso remoto a dispositivos electrónicos y que a partir del hackeo a sus bases de datos internas y la publicación de más de 400GB de información, pudo conocerse la existencia de relaciones comerciales de esta empresa con gobiernos de distintas regiones del mundo e incluso con regímenes autoritarios sancionados por la comunidad internacional. La presencia de Hacking Team en América Latina también es muy fuerte, en países como México, Chile, Colombia, Ecuador, Honduras y Panamá, llegando además a sostener ciertas conversaciones en Argentina.[2]

[2] ADC Alerta: Software de interceptación y vulneración a los derechoshumanos. Agosto 2015. Disponible en (PDF): http://www.adc.org.ar/wp-content/uploads/2015/08/Software-de-

Pero Hacking Team es solo una de las participantes dentro de un negocio mucho más grande y multimillonario dedicado a la comercialización de software de interceptación de comunicaciones y vigilancia. Así podemos nombrar a la empresa estadounidense Blue Coat, una de las empreas que distribuye sus productos a la NSA[3] y también con presencia en Argentina;[4] Gamma International, una empresa anglo-germana conocida por su solución de software FinFisher, también llamado FinSpy; la empresa francesa Vupen Security; la empresa israelí NSO Group, conocida competidora de Hacking Team, con su software Pegasus; y la empresa alemana Utimaco.

La facilidad al acceso de herramientas de vigilancia, así como también a técnicas y herramientas de hacking, es una cuestión que debemos analizar como bidireccional. En este sentido, las agencias y dependencias gubernamentales, así como las corporaciones privadas, tienen la posibilidad de adquirir sin demasiados problemas burocráticos o barreras legales este tipo de productos, aún cuando los adquieran a precios que lejos están de ser irrisorios. Esta circunstancia también tiene incidencia en el esquema de relación entre Estados "contrarios" (para ilustrarlo, sirve el ejemplo USA – Rusia, o Corea del Sur – Corea del Norte) y de las empresas privadas que compiten entre sí por esta "clientela".

Una de las consecuencias directas de este juego de relaciones generado por la facilidad en el acceso y adquisición de estas tecnologías es el alto riesgo para todas las partes involucradas. En el año 2010, investigadores descubrieron que la central nuclear de Irán había sido el blanco de un ataque por medio de un malware[5] conocido como Stuxnet, el cual fue posteriormente atribuido a Estados Unidos e Israel.[6] A comienzos de 2015, Corea del Sur apuntó contra Corea

interceptacion-y- DDHH.-Informe-ADC.pdf

[3] Vaughan-Nichols, Steven J. "How the NSA, and your boss, can intercept and break SSL", junio 2013. Disponible en: http://www.zdnet.com/article/how-the-nsa-and-your-boss-can-intercept-and-break-ssl/

[4] Blue Coat Argentina https://www.bluecoat.com/es/node/1316

[5] El malware es un software malicioso, creado con la intención de introducirse de forma subrepticia en los computadores y causar daño a su usuario o conseguir un beneficio económico a sus expensas.

[6] Zetter, Kim. "An Unprecedented Look at Stuxnet, The World's First Digital Weapon", Wired, noviembre 2014. Disponible en: https://www.wired.com/2014/11/countdown-to-

del Norte como el responsable de los ataques informáticos contra las plantas nucleares del país.[7] Estos son tan solo dos casos dentro del gran número de ataques reportados que surgen año tras año, dentro de lo cual debemos también considerar al sector privado.[8]

Es en este escenario complejo en el que se evidencia el papel fundamental de la ciberseguridad en relación a la protección de las infraestructuras que manejan información y datos sensibles, ante las cuales una posible vulneración o ataque afectaría directamente a la sociedad y la economía.

III Definiendo la ciberseguridad

Al analizar qué se entiende por ciberseguridad, descubrimos entonces tres aspectos en los cuales podríamos dividir el enfoque de la definición, que varían de acuerdo a los fines de quien hace uso del término.

1. **Ciberseguridad como la protección o defensa de las infraestructuras de organismos (públicos y privados), sus redes, datos y usuarios;**
2. **Trabajo que realizan las fuerzas de seguridad en investigación, prevención y acción contra delitos en el ámbito digital (cibercrimen);**
3. **Actividad de vigilancia llevada a cabo por los organismos de inteligencia.**

Podemos hacer esta triple distinción ya que aún no hay un concepto definido de lo que es ciberseguridad a nivel global, ni mucho menos a nivel regional en América Latina.

---

zero-day-stuxnet/

[7] Kwaak, Jeyup S. "North Korea Blamed for Nuclear-Power Plant Hack", The Wall Street Journal, marzo 2015. Disponible en: http://www.wsj.com/articles/north-korea-blamed-for-nuclear-power-plant-hack-1426589324

[8] Al respecto puede consultarse el reporte "Data Breach Investigations Reports" de la firma Verizon, disponible en: http://www.verizonenterprise.com/verizon-insights-lab/dbir/

Aún así, organismos internacionales han avanzado en la discusión sobre el tema ensayando sus propias definiciones.

La Unión Internacional de Telecomunicaciones (UIT), organismo especializado de la Organización de las Naciones Unidas (ONU) para las tecnologías de la información y la comunicación, determinó una definición de ciberseguridad en la Recomendación UIT-T X.1205,[9] luego aprobada con la Resolución 181.[10] La Recomendación establece (el resaltado es propio):

> "La ciberseguridad es el conjunto de *herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, practicas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno*. Los activos de la organización y los usuarios son los dispositivos informáticos conectados, los usuarios y los servicios/aplicaciones, los sistemas de comunicaciones, las comunicaciones multimedias, y la totalidad de la información transmitida y/o almacenada en el ciberentorno. La ciberseguridad garantiza que se alcancen y mantengan las propiedades de seguridad de los activos de la organización y los usuarios contra los riesgos de seguridad correspondientes en el ciberentorno. Las propiedades de seguridad incluyen una o más de las siguientes: disponibilidad; integridad, que puede incluir la autenticidad y el no repudio; confidencialidad".

La Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos (CIDH), de la Organización de los Estados Americanos (OEA), estableció en su publicación "Libertad de expresión e Internet" que "*El concepto de ciberseguridad suele emplearse como un término amplio para referirse a diversos temas*, desde la seguridad de la infraestructura nacional y de las redes a través de las cuales se provee el servicio de Internet, hasta la seguridad

[9] UIT. Recomendación UIT-T X.1205. Abril de 2008. Disponible en: https://www.itu.int/rec/T-REC- X.1205-200804-I/es

[10] UIT. Resolución 181. Noviembre de 2010. Disponible en: https://www.itu.int/net/itunews/issues/2010/09/20- es.aspx

o integridad de los usuarios. No obstante, desarrollos posteriores sugieren la *necesidad de limitar el concepto exclusivamente al resguardo de los sistemas y datos informáticos*. (...) este enfoque acotado permite una mejor comprensión del problema así como una adecuada identificación de las soluciones necesarias para proteger las redes interdependientes y la infraestructura de la información"[11] (el resaltado nos pertenece).

Como también mencionó la Relatoría, lo que se busca evitar con un enfoque acotado en el concepto de ciberseguridad es la posible criminalización del uso de Internet, motivo por el cual "(...) la respuestas de los Estados en materia de seguridad en el ciberespacio debe ser limitada y proporcionada, y procurar cumplir con fines legales precisos, que no comprometan las virtudes democráticas que caracterizan a la red".

Cabe destacar que si bien la OEA tiene un Programa de Seguridad Cibernética, bajo la órbita del Comité Interamericano contra el Terrorismo (CICTE), con el objetivo de –entre otras cosas– ayudar a los Estados miembros a adoptar estrategias nacionales de seguridad cibernética, no brinda un concepto propio de ciberseguridad, por más que sus informes desarrollan el tema en relación a buenas prácticas y reportes regionales sobre el estado de la ciberseguridad.

En el continente americano son varios los países que ya han implementado políticas nacionales de ciberseguridad o están trabajando en ellas. Canadá[12] plantea como eje para su estrategia de ciberseguridad no solo asegurar los sistemas de información gubernamentales y mantener alianzas que los ayudan a asegurar sistemas externos al gobierno, sino también ayudar a sus ciudadanos a navegar y hacer un uso seguro de Internet, dentro de lo cual incluye pelear contra el cibercrimen. Esto implica equipar a las fuerzas de seguridad con recursos modernos y obligar a los proveedores de Internet a que mantengan sistemas de intercepción para que se les pueda solicitar, mediante orden judicial, interceptar las comunicaciones de un determinado objetivo dentro del marco de una

[11] OEA. CIDH. Libertad de expresión e Internet. 31 de diciembre de 2013. Disponible en (PDF): https://www.oas.org/es/cidh/expresion/docs/informes/2014_04_08_internet_web.pdf

[12] Public Safety Canada. Cyber Security Strategy. Disponible en (PDF): http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/cbr-scrt-strtgy-eng.pdf

investigación, además de brindar información sobre sus usuarios.

Si vamos al caso de países europeos, Francia[13] por ejemplo también trabaja en base a un concepto amplio de ciberseguridad, ya que no solo está enfocado a la protección contra vulnerabilidades de aquellos sistemas que almacenan, procesan y transmiten datos, sino también a hacer uso de las técnicas de los sistemas de seguridad de la información para combatir el cibercrimen y establecer la ciberdefensa del país.

Como podemos observar, el término ciberseguridad es utilizado en forma absolutamente flexible. Sin una definición acordada internacionalmente, la manera en la que sea enmarcada dependerá de quien se encuentre desarrollando sus políticas. Desde la protección de la información en manos del Estado y del sector privado, así como resguardar la seguridad de los servicios a los que acceden los ciudadanos online, hasta la persecución de delitos informáticos y el desarrollo de la ciberdefensa y sistemas de inteligencia del país, los alcances de la ciberseguridad dependerán del contexto y factores específicos de quien hace uso del término.

Como mencionamos en el capítulo anterior, las problemáticas que enfrentan determinados países hacen que deban tomar medidas que en ocasiones son radicalmente opuestas entre naciones. A esto, debe sumarse que en muchos países quienes mueven la agenda política son unos pocos funcionarios del gobierno de turno, y muchas veces se pierde la oportunidad de discutir en un contexto verdaderamente democrático cuál es el mejor camino a tomar en torno a una temática como la ciberseguridad.

i (Des)militarizando concepciones: alineando la ciberseguridad con los derechos humanos

A comienzos de abril de 2016, un conjunto de organizaciones de la sociedad civil de América Latina nos unimos para firmar una declaración respecto a diez puntos fundamentales que entendemos deben ser impulsados localmente buscando

[13] UIT. Estrategias Nacionales de Ciberseguridad. Francia. Disponible en (PDF): http://goo.gl/ksfhou

alcanzar la alineación de las políticas de ciberseguridad con una perspectiva de derechos humanos.[14]

Reproducimos algunas de las recomendaciones efectuadas en la declaración a continuación:

- Cualquier estrategia de ciberseguridad debe estar alineada con las normativas de derechos humanos del país que las implementa, del sistema interamericano y de estándares internacionales (en este sentido, un buen ejemplo para tener como guía son los Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones). Es fundamental prestar especial atención a la protección de los derechos a la libertad de expresión, la privacidad y la libre asociación, los cuales –como venimos analizando– pueden ser vulnerados fácilmente si no son puestas a consideración las implicancias de la implementación y uso de ciertas tecnologías o prácticas.

- Debido a que el concepto ciberseguridad responde a una raigambre fuertemente militar, se recomienda sustituirla por el termino seguridad digital, el cual debe tener en su núcleo la protección de la ciudadanía, la persona y sus comunidades, a la vez de que se busca promover el desarrollo económico y social, respetando las instituciones democráticas, el Estado de derecho y los derechos fundamentales de los ciudadanos. Logrando poner un límite al concepto que trasciende el ambiente militar, de defensa y de inteligencia.

- Para que todo el camino recorrido a lo largo del desarrollo e implementación de las políticas de seguridad digital sea efectivo, debemos alentar a los gobiernos a que presten especial atención al uso de productos que cumplan con estándares reconocidos de seguridad digital, ya que de lo contrario, se dejaría abierta la puerta a posibles vulnerabilidades y riesgos que pondrían en peligro lo plasmado en las políticas y estrategias de seguridad digital.

[14] ADC Digital, "OEA: Declaración de sociedad civil lationamericana sobre seguridad digital", abril 2016. Disponible en: https://adcdigital.org.ar/2016/04/06/oea-declaracion-sociedad-civil-latinoamericana-seguridad-digital/

IV Tendencias internacionales en el desarrollo de políticas de ciberseguridad y su adecuación al contexto latinoamericano

Al comenzar a buscar referencias de organismos internacionales que estudian la ciberseguridad dentro de un contexto de políticas públicas y su impacto social, nos encontramos con una baja cantidad de casos que pudiéramos analizar y trasladar a los fines del presente informe.

Por una parte, elegimos un estudio desarrollado por la Organización para la Cooperación y el Desarrollo Económico (OCDE) que analiza distintas estrategias nacionales de ciberseguridad desde un punto de vista de la economía de Internet. La OCDE es un foro en el que los países miembros pueden compartir experiencias sobre políticas y buscar soluciones a problemáticas comunes. Si bien Argentina no forma parte de la OCDE, este informe es una buena mirada a la realidad de distintos países, principalmente de América del Norte y Europa, y cómo los mismos afrontan la temática de la ciberseguridad, cómo es incluida la misma en las políticas públicas y en qué problemáticas debe estar enfocada. Otro de los motivos por el que elegimos este informe es el hecho de que se hayan sumado la perspectiva, análisis y recomendaciones de actores no gubernamentales miembros de la OCDE.

Por otra parte, pasando al contexto latinoamericano, explicamos algunos aspectos de la situación que vivencia Colombia en el desarrollo de sus políticas de ciberseguridad, desde que se convirtió en el primer país de América Latina en adoptar una estrategia nacional a través del documento Conpes 3701 de julio de 2011, conocido como "Lineamientos de política para la Ciberseguridad y Ciberdefensa", además de las observaciones realizadas por un grupo de expertos convocados por la OEA a pedido del gobierno colombiano para analizar el caso del país y en base a eso realizar recomendaciones para la implementación y desarrollo de la estrategia.

Finalmente, cerramos este capítulo con dos reportes de la OEA respecto a la situación en la que se encuentran los países de América Latina en el desarrollo

de estrategias y políticas de ciberseguridad, de los cuales resaltamos las observaciones que se realizan sobre el caso de la Argentina.

i Una nueva generación de estrategias nacionales de ciberseguridad para la economía de Internet

A fines del año 2012, la Organización para la Cooperación y el Desarrollo Económicos (OCDE) publicó el informe "Elaboración de políticas de ciberseguridad en un punto de inflexión: Análisis de una nueva generación de estrategias nacionales de ciberseguridad para la economía de Internet"[15] (Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy), en el cual se analizan las políticas de ciberseguridad de diez países –Australia, Canadá, Francia, Alemania, Japón, Países Bajos, Reino Unido, Estados Unidos, Finlandia y España– identificando diferencias y similitudes, y comparando las características de los distintos planes de acción de los gobiernos, a la vez de que aprovecha a poner de manifiesto ciertas tendencias en la confección de las políticas de ciberseguridad, además de remarcar recomendaciones de otros actores no gubernamentales, como la comunidad técnica de Internet, el sector privado y la sociedad civil; a continuación nos explayaremos sobre algunos de los descubrimientos, tendencias y recomendaciones más relevantes de este informe.

La ciberseguridad se ha ido elevando dentro de las prioridades de los gobiernos, los cuales han evaluado que, por un lado, Internet y las TICs son esenciales para el desarrollo económico y social, conformando una infraestructura vital para la innovación, el bienestar social y la expresión individual, pero a medida que la economía de Internet crece, la economía y la sociedad entera se vuelven cada día más dependientes de esta infraestructura para poder desarrollar sus actividades. Por otro lado, las amenazas en Internet se encuentran en rápido y constante aumento, no solo alimentadas por actores criminales individuales, sino también

[15] Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy. OCDE, 2012. Disponible en: http://www.oecd.org/sti/ieconomy/comparativeanalysisofnationalcybersecuritystrategies.htm

por Estados extranjeros y grupos políticos que llevan a cabo actos de hacktivismo, ciberespionaje, sabotaje e incluso operaciones militares.

Es por esto que prácticamente todas las estrategias de ciberseguridad analizadas muestran una evolución en el enfoque de la temática, pasando de únicamente proteger a individuos y organizaciones particulares, a proteger a la sociedad en su totalidad.

Debido a que Internet se ha vuelto cada vez más esencial para el pleno desarrollo de la economía y la sociedad, las consecuencias que pueden acarrear las fallas de seguridad pueden afectar directamente a toda la sociedad, por lo que las estrategias de ciberseguridad se centran en dos objetivos primordiales: "el fortalecimiento de la ciberseguridad para la economía de Internet para impulsar aún más la prosperidad económica y social, y la protección de las sociedades dependientes del ciberespacio frente a las amenazas cibernéticas".

El hecho de que Internet se haya convertido en una herramienta vital para la economía moderna tiene varias consecuencias en la formulación de políticas de ciberseguridad, siendo una de las principales la adopción de políticas que tratan a la ciberseguridad en forma integrada y global. Los gobiernos reconocen la necesidad de abordar todas las facetas de la ciberseguridad de manera holística, abarcando aspectos sociales, educativos, legales, económicos, técnicos, diplomáticos, militares y de inteligencia, así como también vinculados a las fuerzas de seguridad. De acuerdo a la OCDE, este tipo de enfoque debe ser apoyado mediante un liderazgo fuerte, en general a la cabeza del Estado o jefes de gobierno.

No todas las estrategias utilizan los términos "ciberseguridad" o "ciberespacio", aún así, la OCDE señala que las estrategias que sí utilizan este término, brindan una definición, que varía de acuerdo a cada país ya que se ve modificada con los matices propios del tipo de política que se pretende adoptar.

Por otra parte, hay algunos conceptos que las estrategias de distintos países comparten, como ser:

- Coordinación gubernamental mejorada a nivel político y operativo: Ningún organismo puede argumentar que tiene una comprensión global o completa,

ni una autoridad lo suficientemente amplia, como para gestionar todas las facetas de la ciberseguridad. Por ello, es fundamental la coordinación entre los organismos pertinentes, las estrategias asignan claramente las responsabilidades de cada uno de ellos para fomentar la proactividad y evitar la duplicación.

- Cooperación público-privada reforzada: Todas las estrategias reconocen que Internet está fundamentalmente en manos del sector privado, sea como propietarios, a nivel operativo o ambos. En tal sentido, reconocen que las políticas se deben basar en convenios público-privados inclusivos o multidisciplinarios, que comprenda la participación de la sociedad civil, las empresas, la comunidad técnica y la academia.

- Cooperación internacional mejorada: La mayoría de las estrategias comparten como objetivo la necesidad de mejorar las alianzas internacionales con países o aliados afines, nombrando organizaciones como el Consejo de Europa, la Unión Europea, el G8, el Foro de Gobernanza de Internet, la OCDE y las Naciones Unidas (incluyendo la Unión Internacional de Telecomunicaciones), pero en general sin ofrecer mucho detalle respecto al rol que desearían que las mismas cumpliesen. La OCDE resalta a su vez que varios países mencionan a la Organización del Tratado del Atlántico Norte (OTAN) respecto a la ciberseguridad en un contexto militar.

- Respeto por los valores fundamentales: Todas las estrategias enfatizan la necesidad de que las políticas de ciberseguridad respeten los valores fundamentales, dentro de los cuales incluyen la privacidad, la libertad de expresión y el libre flujo de información. A la vez que remarcan explícitamente la necesidad de mantener la apertura y la libertad características de Internet.

Una de las tendencias más relevantes que encontró la OCDE es que *la mayoría de las estrategias de ciberseguridad comenzaron a poner particular énfasis en consideraciones de soberanía, incluyendo de esta manera aspectos militares, de seguridad nacional, de inteligencia y de defensa*, al momento del desarrollo de sus políticas.

Esta evolución en el enfoque de las estrategias, remarca la OCDE, es una consecuencia directa de la consideración de que la ciberseguridad se refiere a la protección de la sociedad en su totalidad, esto lleva a que los gobiernos requieran poner en práctica un enfoque integral.

Las consideraciones de soberanía surgen en distintos niveles de la política nacional, respecto a lo cual la OCDE da algunos ejemplos basados en las políticas estudiadas:

- A nivel estratégico: se reconoce el riesgo de los ciberataques dirigidos hacia militares y la infraestructura del estado, o el ciberespionaje patrocinado por Estados extranjeros.
- A nivel organizacional: distintos departamentos y ministerios a cargo de las actividades militares y de inteligencia comenzaron a ser incluidos en la coordinación gubernamental para la elaboración de las políticas de ciberseguridad.
- A nivel operativo: los cuerpos de inteligencia comienzan a tomar un rol más primario, al convertirlos en fuente de información para el conocimiento de la situación.

Por otra parte, la OCDE encontró que la mayoría de las estrategias comprende a su vez un plan de acción que apunta al fortalecimiento de determinadas áreas identificadas por el gobierno como aquellas sobre las cuales se necesita trabajar para lograr una infraestructura de ciberseguridad robusta. La OCDE determinó que estas áreas son, generalmente:

- La seguridad del gobierno: respecto a la infraestructura que es utilizada a nivel estatal.
- La protección de las infraestructuras críticas de la información.
- La lucha contra el cibercrimen.
- La concientización: se busca generar iniciativas dirigidas a los sectores más vulnerables de la sociedad, por ejemplo, los niños, niñas y adolescentes.

- La educación: los planes de acción reconocen la necesidad de una fuerza laboral fuerte en materia de ciberseguridad, y remarcan el desarrollo de habilidades de ciberseguridad como una prioridad clave.

- Respuesta: las estrategias reconocen el papel fundamental desempeñado por los equipos de respuesta a incidentes informáticos (Computer Security Incident Response Team, o CSIRT), creando uno a nivel nacional o reforzando el existente a través del plan de acción.

Finalmente, la OCDE agrega a su reporte algunas recomendaciones aportadas por actores no gubernamentales (participaron: Business and Industry Advisory Committee (BIAC), Civil Society Internet Society Advisory Council (CSISAC) y Internet Technical Advisory Committee (ITAC)). Estos –en general– coinciden en que la colaboración de múltiples partes interesadas (conocido como modelo multistakeholder) y la cooperación, son los mejores medios para desarrollar políticas de ciberseguridad efectivas que respeten la naturaleza fundamentalmente global y abierta de Internet; por otra parte, las políticas de ciberseguridad deben ser lo suficientemente flexibles para adaptarse a la naturaleza dinámica de Internet.

Consideramos de importancia remarcar algunas de las sugerencias expresadas por la sociedad civil ante la consulta de la OCDE, fundamentalmente:

- Para evitar que determinadas medidas adoptadas en la estrategia de ciberseguridad se tornen ilegítimas o amenazantes de derechos fundamentales con el avance de la tecnología y las prácticas, se pueden incluir cláusulas de extinción que automáticamente les pongan un fin, actuando como mecanismo de control de los derechos de los ciudadanos.

- Los gobiernos deberían tomar un rol más activo actuando como modelos a seguir, adoptando mejores prácticas y tecnologías que respeten, no solo estándares internacionales de seguridad digital, sino fundamentalmente los derechos fundamentales de las personas. Con la adopción de este rol, los gobiernos pueden proporcionar una dirección clara para el resto de los actores que dependen de la estrategia de ciberseguridad.

- Es fundamental que los responsables a cargo de la elaboración de las políticas de ciberseguridad busquen el asesoramiento de la comunidad técnica de Internet tan pronto como sea posible en el proceso de confección de las políticas; de esta forma se evitaría tomar decisiones erróneas tecnológica y operativamente, que pongan en juego, por ejemplo, la naturaleza misma de Internet.

- Las políticas de ciberseguridad podrían fomentar el desarrollo de estándares abiertos que permitan la innovación de soluciones de seguridad, basándose en grupos de estandarización abiertos y respetados, evitando la modificación unilateral de los estándares de Internet.

ii Colombia: pionera en América Latina

Si bien el reporte publicado por la OCDE comprende el análisis de varios países de Europa y América del Norte, lo cierto es que la realidad de los mismos no necesariamente se condice con el contexto latinoamericano, fundamentalmente a nivel institucional, caracterizada en general por su debilidad. Así por ejemplo, en el caso de Argentina y particularmente en torno a la ciberseguridad, al momento de analizar cómo y por qué se fueron adoptando determinadas políticas públicas, podemos inferir que las mismas parecieran responder más a la adopción de una palabra de moda que a la necesidad real, analizada, consensuada y comprometida de generar un política pública en materia de ciberseguridad. Esto es así pues al analizar el trasfondo de las políticas y prácticas de ciberseguridad a nivel nacional, hemos advertido que las mismas no han sido acompañadas del presupuesto necesario para cumplir con todos los objetivos que se habían planteado o con la estructura que planteaba la normativa, ni fueron pensadas como políticas de Estado a largo plazo. Volveremos sobre este tema.

Por otra parte, un gran número de países latinos cuentan con pasados autoritarios por fuertes dictaduras militares, o que incluso sin llegar a tal punto y aún en democracia tienen una cultura y una presencia militar muy arraigada en sus instituciones, desde los modos de trabajar del Estado hasta la formación de funcionarios y empleados. Este contexto no puede dejarse de lado cuando se

pretende incursionar en el desarrollo de políticas públicas, evolucionando la mirada de las mismas hacia un mayor respeto por los derechos fundamentales y las instituciones democráticas.

Un caso particular es el que se desarrolla en Colombia, donde en el año 2011, a través del documento "Lineamientos de Políticas para Ciberseguridad y Ciberdefensa"[16] del Consejo Nacional de Política Económica y Social (CONPES) se creó una Comisión Intersectorial con el objetivo de fijar la política de ciberseguridad. "Aunque básicamente toda su composición, excepto por el Ministro de Tecnologías de Información y Comunicaciones y Planeación Nacional, tiene relación con el sector defensa, destaca que el Director General de la Dirección Nacional de Inteligencia haga parte de la comisión. No hay nada en el documento CONPES que justifique la presencia de este funcionario" establece Juan Diego Castañeda, abogado de la Fundación Karisma.[17]

"Que la política e institucionalidad de ciberseguridad gire tan fuertemente en torno al Ministerio de Defensa parece estar decidido antes de la creación del CONPES, pues según el mismo documento, después de reuniones en 2008 y 2009 con la OEA, especialmente su Comité Interamericano contra el Terrorismo (CICTE), 'las instituciones del Estado solicitaron al Ministerio de Defensa Nacional asumir un liderazgo nacional que permitiera impulsar políticas en seguridad cibernéticas. (...) El diagnóstico final indicó que el Ministerio de Defensa tenía la mayor capacidad para manejar de manera eficiente y coordinada estos temas.' (CONPES 2011) No hay más justificaciones en este documento", agrega Castañeda.

En abril de 2014, la Organización de los Estados Americanos conformó un consejo de expertos para evaluar el estado de la seguridad cibernética a pedido del gobierno de Colombia, del cual participaron el Consejo de Europa, el Foro Económico Mundial, INTERPOL, las Naciones Unidas, la OCDE y la Universidad de Oxford, quienes emitieron finalmente el documento "Misión de Asistencia

[16] CONPES 3701, Consejo Nacional de Política Económica y Social, República de Colombia, 2011. Disponible en: http://mintic.gov.co/portal/604/articles-3510_documento.pdf

[17] Entrevista con Juan Diego Castañeda, abogado e investigador de Fundación Karisma (https://karisma.org.co). Marzo 2016.

Técnica en Seguridad Cibernética: Conclusiones y recomendaciones".[18] Si bien el mismo está desarrollado desde el punto de vista específico de Colombia, a través de él podemos comprender mejor cuál es la posición de la OEA respecto a determinados puntos que hemos ido mencionado; reproducimos algunos de ellos a continuación.

La OEA establece que la estrategia de ciberseguridad debe contar con una "visión global", la cual debe formular objetivos amplios que determinen por qué son importantes para la nación que los persigue, además de distinguir entre los objetivos de prosperidad económica y social; defensa del país (militar, inteligencia, etc); y lucha contra el cibercrimen.

El marco institucional de ciberseguridad debe contar con un órgano de coordinación permanente, al cual se le asignará un rol que se extienda por todo el gobierno; este organismo debería responder directamente al Presidente. El órgano de coordinación debe contar con la "autoridad y responsabilidad legal suficiente para actuar", incluyendo los recursos presupuestales para responder a la visión global de la ciberseguridad; debe tener la "responsabilidad de dirigir la formulación de la política pública para asegurar un enfoque de conjunto gubernamental coherente"; así como también contar con la "capacidad de desarrollar una evaluación integral de los riesgos de ciberseguridad nacional". El órgano coordinador "debe ser un repositorio de mejores prácticas de ciberseguridad (...) incluida la orientación y el asesoramiento sobre las normas y marcos para la acreditación y la certificación".

Por otra parte, la OEA también establece como una parte fundamental del desarrollo de las políticas el vínculo integral con todas las partes interesadas, "Es esencial involucrar a todos los actores (públicos y privados) en el desarrollo de la visión, las políticas y en su implementación, para maximizar su compromiso". En tal sentido, se debe consultar con todas las partes (sociedad civil, comunidad técnica, sector privado, academia, entidades internacionales) la forma de organizar el diálogo sistemático entre las mismas, establecer reglas de consulta sis-

[18] Misión de Asistencia Técnica en Seguridad Cibernética, Organización de los Estados Americanos, abril de 2014. Disponible en: http://www.oas.org/documents/spa/press/Recomendaciones_COLOMBIA_SPA.pdf

temática tanto en la fase inicial como a lo largo de la elaboración de las políticas, y desarrollar un plan a corto, mediano y largo plazo para llegar progresivamente a todos los actores gubernamentales y no gubernamentales.

Respecto a la persecución de los delitos informáticos, la OEA recomienda que se mantengan adecuadamente separados de las cuestiones de ciberdefensa y ciberguerra, "definiendo la unidad policial que se va a encargar específicamente de la prevención, investigación y persecución de los delitos informáticos".

La OEA destaca que se debe tener especial consideración por las pequeñas y medianas empresas y sectores con pocos recursos financieros para desarrollar capacidades de ciberseguridad, a los cuales se puede ayudar a través de, por ejemplo, incentivos fiscales o subvenciones.

Finalmente, debido a que la ciberseguridad involucra necesariamente a múltiples actores de la sociedad, para alcanzar una labor eficaz "se requiere una cooperación profunda y sostenida con el sector privado (nacional e internacional), así como los gobiernos extranjeros, organizaciones internacionales y expertos académicos".

"La OEA, por lo menos en estas recomendaciones, no parece señalar la necesidad de desligar la ciberseguridad del Ministerio de Defensa. Solo aclara que se necesita un organismo coordinador independiente. En inteligencia, recomienda separar objetivos económicos y sociales, de defensa y de lucha contra el crimen", comenta Castañeda.

"En cuanto a los cambios que nos preocupa que se realicen en nombre de la ciberseguridad" agrega Castañeda, "están:

- La ampliación de poderes militares, inteligencia y policía, sin la ampliación y mejora de controles;
- La ampliación de la retención de datos a Internet;
- El uso de herramientas de hacking para hacer intrusión en dispositivos, sin debate ni control de ningún tipo;
- La ampliación de poderes y técnicas de interceptación de comunicaciones y monitoreo del espectro;

- La regulación del cifrado;
- El destino de amplios presupuestos que tengan como prioridades los opuestos a la necesidad de mantener sistemas informáticos actualizados y resilientes, y a capacitaciones que no incluyan visiones diferentes de la militar".

En el informe "Libertad de Expresión e Internet" la Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos, refirió que "la respuesta de los Estados en materia de seguridad en el ciberespacio debe ser limitada y proporcionada, y procurar cumplir con fines legales precisos, que no comprometan las virtudes democráticas que caracterizan a la red" (Párrafo 120, página 59). En tal sentido, "las políticas públicas en materia de ciberseguridad deben ser proporcionales al riesgo que enfrentan y, en cualquier caso, deben sopesar el objetivo de seguridad y la protección de los derechos fundamentales" (Párrafo 124, página 60).

A su vez, "las autoridades deben informar y rendir cuentas sobre las medidas tomadas en materia de ciberseguridad, tanto de aquellas directamente implementadas como de las que ejecutan intermediarios privados contratados por el Estado" (Párrafo 126, página 61). "Los programas oficiales y las políticas públicas de ciberseguridad deben contar con mecanismos de supervisión y control cuya instancia máxima sea un juez. De la misma manera, debe haber procedimientos de seguimiento con algún grado de participación de la sociedad civil" (Párrafo 128, página 61).

iii La ciberseguridad en el contexto lationamericano desde la OEA

Como hemos venido exponiendo, la OEA fue uno de los organismos pioneros en tratar la temática de la ciberseguridad desde un marco regional –dada su naturaleza–; dada la relevancia de este organismo para los países del continente, consideramos de relevancia mencionar en este informe dos de sus más recientes trabajos: "Reporte de Seguridad Cibernética e Infraestructura Crítica

de las Américas" y "Ciberseguridad: ¿Estamos preparados en América Latina y el Caribe?".

El primer informe, "Reporte de Seguridad Cibernética e Infraestructura Crítica de las Américas", fue realizado en conjunto con Trend Micro, es un estudio elaborado a partir de una encuesta efectuada a entes gubernamentales e industrias críticas como las comunicaciones, banca y finanzas, manufactura, energía y seguridad, de 20 de los países miembros de la OEA, con el fin de brindar un panorama sobre el estado de situación de la seguridad digital respecto de las infraestructuras críticas de la región y las amenazas que enfrentan las organizaciones, así como también de las medidas y políticas de seguridad cibernética de las organizaciones, colaboración con gobiernos locales y la preparación para enfrentar ataques cibernéticos.

Algunas de las conclusiones del reporte mostraron que:

- Los ataques dirigidos a la infraestructura son un peligro claro y presente. Sólo un menor porcentaje de los entrevistados pudo decir que no habían visto este tipo de ataques. Por otra parte, aseguraron que las amenazas están siendo muy severas, la frecuencia de los ataques va en aumento y estos cada vez más sofisticados. Según algunos entrevistados, el panorama a futuro es desalentador cuando se trata de la protección de las infraestructuras críticas.

- Existe una falta de asociación proactiva entre los gobiernos y las organizaciones privadas en la región. Una escueta mayoría de los entrevistados informaron que no hay un diálogo entre estos sectores, o que en caso de haberlo, el diálogo es puramente informal.

- Los presupuestos que manejan las organizaciones se presentan como un impedimento al momento de necesitar recursos para defender continuamente los ataques dirigidos contra sus infraestructuras.

- La falta de financiamiento y de liderazgo gubernamental enfocada en ciberseguridad deja a los defensores de las infraestructuras sintiéndose cada vez más solos. La OEA establece finalmente que los gobiernos de la región

necesitan tender una mano a los encargados de la infraestructura crítica que buscan ayuda y guiarlos para ofrecer mejor protección contra los crecientes ataques a este sector crucial.

El segundo informe, "Ciberseguridad: ¿Estamos preparados en América Latina y el Caribe?", elaborado por el Observatorio de la Ciberseguridad en América Latina y el Caribe mediante una colaboración, entre el Banco Interamericano de Desarrollo y la OEA, busca presentar un panorama completo y actualizado sobre el estado de la seguridad cibernética en la región, a través de la recolección de datos de distintos actores como son: agencias gubernamentales, operadores de infraestructuras críticas, las fuerzas militares, la policía, el sector privado, la sociedad civil y la academia. El informe consta de dos secciones, la primer parte consta de distintos ensayos elaborados por expertos en la temática sobre las tendencias en la región; la segunda parte es el reporte de los distintos países estudiados, presentando una visión general sobre el estado de la ciberseguridad en los mismos.

Las reflexiones a las que arribaron desde el BID muestran las tendencias que han comenzado a surgir en la región:

- Si bien los gobiernos reconocen que es importante asegurar un acceso asequible a Internet y TICs, para lograr innovación empresarial, crecimiento y un mayor desarrollo en la prestación de servicios públicos, la penetración de Internet es aún muy baja en aproximadamente la mitad de la región.

- Adoptar una estrategia nacional de ciberseguridad es un elemento fundamental para el compromiso de un país en asegurar la infraestructura cibernética, servicios y ambiente de negocios de los que dependen su futuro y el bienestar económico. Los países que han establecido políticas de seguridad cibernética formalmente son: Brasil, Colombia, Jamaica, Panamá, Trinidad y Tobago, y Uruguay.

- En gran medida, hay un desconocimiento por parte de la sociedad sobre los riesgos y las vulnerabilidades asociadas con el uso de las TICs. El BID

destaca la importancia de los gobiernos de describir los riesgos y las oportunidades asociadas con el aumento de la conectividad y la dependencia de Internet.

- Si bien la mayoría de las autoridades nacionales mantienen líneas de comunicación abiertas y activas, así como una colaboración con los sectores críticos y empresas clave, aún hay desconfianza entre las partes interesadas que implica una disminución en la colaboración.

- La respuesta a crisis o los mecanismos de presentación de informes se encuentran aún en una etapa inicial en la región. La capacidad para abordar proactivamente las amenazas cibernéticas es limitada. Aproximadamente la mitad de los países de la región han establecido y puesto en marcha Equipos de Respuesta a Incidentes de Seguridad Informática (también conocidos como CERT).

- En toda la región se encuentran esfuerzos en el desarrollo de marcos legales integrales para combatir el cibercrimen.

- Algunos gobiernos, aprovechando su mayor conectividad a Internet, se encuentran explorando oportunidades en el desarrollo de tecnología, en la ampliación de su industria interna de tecnología, así como poner en marcha programas cibernéticos de investigación y desarrollo.

Al final del próximo capítulo ahondaremos en los análisis específicos que realizan los informes de Trend y del BID sobre la situación de la Argentina, comparándolo con lo que hemos podido observar a partir de la investigación para el presente documento.

V En busca de una agenda de ciberseguridad en Argentina

Los primeros pasos dados en esta investigación nos mostraron que el término ciberseguridad aparece inserto en alguna normativa, utilizado en forma frecuente

en los últimos años, pero las mismas no brindan ningún tipo de definición o conceptualización sobre qué es en sí la ciberseguridad.

Para poder comprender con mayor claridad la situación particular de la Argentina, es necesario desarrollar el recorrido de la evolución normativa bajo la cual se fue llevando la temática a la agenda pública.

i Coordinación de Emergencia en Redes Teleinformáticas de la Administración Pública Argentina (ArCERT)

En el año 1999, a través de la Resolución N°81/99, fue creada esta Coordinación dentro de la ex-Secretaría de la Función Pública, dependiente de la Jefatura de Gabinete de Ministros, en virtud de la facultad de establecer la política sobre tecnologías referidas a informática, teleinformática o telemática, multimediales y de telecomunicaciones asociadas con lo informático para el Sector Público Nacional.[19]

Esto así pues, según reza la Resolución, el Estado Nacional había logrado notables avances en la incorporación de tecnologías informáticas y de comunicaciones en sus organismos, la interconexión de éstos y el desarrollo de redes, con el consecuente incremento de la información que circulaba por las redes de la Administración Pública Nacional, además del aumento en la complejidad de la interconectividad entre redes, producido en gran medida por la utilización de Internet, por lo que resultaba necesario dotar a la Administración Pública Nacional de un servicio de respuesta ante los incidentes que pudieran manifestarse en sus redes.

De tal suerte, alguno de los objetivos del ArCERT fueron: promover la coordinación entre las unidades de administración de redes informáticas para la prevención, detección, manejo y recopilación de información sobre incidentes de seguridad; proponer normas; asesorar técnicamente ante incidentes de seguridad en sistemas informáticos, centralizar reportes sobre incidentes de seguridad;

[19] Resolución N°81/1999. Disponible en: http://www.infoleg.gob.ar/infolegInternet/anexos/55000-59999/58799/norma.htm

actuar como repositorio de toda la información sobre incidentes de seguridad, herramientas, técnicas de protección y defensa, etc.

La ArCERT pasó, luego, a integrar el Programa ICIC.

ii Programa de Infraestructuras Críticas de Información y Ciberseguridad (ICIC)

El ICIC[20] es creado en el año 2011, mediante la Resolución N°580/11 de la Jefatura de Gabinete de Ministros.[21]

Las razones de la creación de dicho programa están explicadas en los considerandos de la Resolución, que entre otras cuestiones destaca que la infraestructura digital de la que depende la utilización de las comunicación virtuales, es una infraestructura crítica y por ello imprescindible para el funcionamiento de los sistemas de información y comunicaciones, que a su vez dependen de modo inexorable del Sector Público Nacional y del sector privado.

La resolución destaca también que la seguridad de la infraestructura digital se encuentra expuesta a constantes amenazas, que en caso de materializarse pueden ocasionar graves incidentes en los sistemas de información y comunicaciones, por lo que resulta imprescindible adoptar las medidas necesarias para garantizar el adecuado funcionamiento de las infraestructuras críticas. Por ello deviene imprescindible la creación y adopción de un marco regulatorio específico que propicie la identificación y protección de las infraestructuras estratégicas y críticas del Sector Público Nacional, los organismos interjurisdiccionales y las organizaciones civiles y del sector privado que así lo requieran, y la colaboración de los mencionados sectores con miras al desarrollo de estrategias y estructuras adecuadas para un accionar coordinado hacia la implementación de las pertinentes tecnologías, entre otras acciones.

Así se creó el ICIC, que tiene como objetivo general la elaboración de un marco

[20] Sitio web oficial: http://icic.gob.ar

[21] Resolución N°580/2011. Disponible en: http://www.infoleg.gob.ar/infolegInternet/anexos/185000-189999/185055/norma.htm

regulatorio específico que propicie la identificación y protección de las infraestructuras estratégicas y críticas de las entidades y jurisdicciones de todo el sector público nacional, los organismos interjurisdiccionales, y las organizaciones civiles y del sector privado que así lo requieran, así como al fomento de la cooperación y colaboración de los mencionados sectores con miras al desarrollo de estrategias y estructuras adecuadas para un accionar coordinado hacia la implementación de las pertinentes tecnologías.

A tal fin, ICIC deberá elaborar y proponer normas, colaborar con el sector privado, administrar información sobre reportes de incidentes de seguridad en el Sector Público Nacional y encausar posibles soluciones en forma organizada y unificada, establecer prioridades y planes estratégicos para liderar el abordaje de ciberseguridad, alertar sobre casos de detección de intentos de vulneración de infraestructuras críticas, coordinar la implementación de ejercicios de respuesta, asesorar técnicamente ante incidentes de seguridad reportados, centralizar reportes, actuar como repositorio, elaborar un informe anual de la situación en materia de ciberseguridad para su publicación abierta y transparente, monitorear los servicios que el Sector Público Nacional brinda a través de la red de Internet y aquellos que se identifiquen como infraestructura críticas para prevención de posibles fallas de ciberseguridad, promover concientización acerca de los riesgos que genera el uso de medios digitales, difundir información útil para incrementar los niveles de seguridad de las redes, entre otros.

Es dable destacar que para participar en el Programa los organismos interesados, sean del Sector Público Nacional, organismos interjurisdiccionales, organizaciones de sociedad civil y/o del sector privado, deben manifestar su adhesión al mismo.

Asimismo, la Resolución establece que el ICIC no interceptará ni intervendrá en conexiones o redes de acceso privado, en cumplimiento de lo estipulado por la Ley de Protección de Datos Personales y normativa reglamentaria vigente.

El ICIC cuenta con cuatro grupos de trabajo:

1. ICIC CERT: para hacer frente a las emergencias informáticas;
2. Grupo de Acción Preventiva (GAP): para la investigación y análisis de nuevas tecnologías y herramientas informáticas;

3. Grupo de Infraestructuras Críticas de Información (GICI): para la identificación y análisis de las infraestructuras críticas del país, como son las telecomunicaciones, la energía, el petróleo, el gas y los servicios financieros;

4. Internet Sano: para la concientización de los riesgos del uso de medios digitales en el Sector Público Nacional.

A través del Instituto Nacional de la Administración Pública (INAP), el ICIC brinda cursos, talleres y charlas enfocadas en la estrategia de capacitación diseñada por la Oficina Nacional de Tecnologías de la Información (ONTI). En julio de 2014, por ejemplo, se llevó a cabo la capacitación titulada "Introducción a las infraestructuras críticas de información y ciberseguridad" con una modalidad de tipo virtual o a distancia, orientada a los agentes de entidades y jurisdicciones que componen el Sector Público Nacional a cargo de tareas administrativas, al personal de organismos interjurisdiccionales, al personal de organismos civiles y al personal del sector privado.

Esta capacitación se dividió en tres módulos, en los cuales, además de las bases teóricas sobre el tema (¿Qué son las infraestructuras críticas? ¿Qué se considera ciberseguridad?), se trataron los casos específicos de la Unión Europea con la Agencia Europea para la Seguridad de la Información y la Red (ENISA, por sus siglas en inglés), así como las estrategias de la ciberseguridad nacional del Reino Unido, Canadá, España, Estados Unidos y Alemania.

Al momento de su creación, la autoridad de aplicación del Programa ICIC era la Oficina Nacional de Tecnologías de Información (ONTI),[22] dependiente de la Subsecretaría de Tecnologías de Gestión de la Secretaría de de Gabinete de la Jefatura de Gabinete de Ministros.

La ONTI es la Oficina encargada de la implementación de estrategias de innovación informática de la Administración Pública, desarrolla los sistemas que son utilizados en procedimientos de gestión, fija los estándares que deben utilizar los organismos públicos cuando incorporan nuevas tecnologías, colabora con otras dependencias en la creación de portales informativos y de gestión y promueve

[22] Sitio web oficial: http://secretariagabinete.jefatura.gob.ar/ONTI

la interoperabilidad de las redes de información de las instituciones estatales. También coordina las respuestas ante los intentos de ataque o penetración a las redes informáticas de los organismos públicos, fija los estándares de seguridad y controla que sean cumplidos en los sistemas del Estado, además de tener a su cargo implementación y control de uso de la certificación digital en el Estado, que permite tramitar electrónicamente los expedientes.

iii Subsecretaría de la Protección de Infraestructuras Críticas de Información y Ciberseguridad

El Programa ICIC fue uno de los antecedentes para que en el mes de junio de 2015, el Poder Ejecutivo Nacional (PEN) decretara la creación de la Subsecretaría de Protección de Infraestructuras Críticas de Información y Ciberseguridad, dependiente de la Secretaría de Gabinete de la Jefatura de Gabinete de Ministros, con el principal objetivo de llevar a cabo la estrategia nacional de protección de infraestructuras críticas de información y ciberseguridad.

Así lo estableció el Decreto N°1067/2015 del PEN, esgrimiendo como fundamentación el perfeccionamiento de la utilización de los recursos públicos con miras a una mejora sustancial en la calidad de vida de los ciudadanos, focalizando su accionar en la producción de resultados que sean colectivamente compartidos y socialmente valorados.

Para ello estimó necesario establecer una nueva conformación organizativa de los niveles políticos, basado en criterios de racionalidad y eficiencia que posibiliten una rápida respuesta a las demandas de la sociedad, dando lugar a estructuras dinámicas y adaptables a los cambios permanentes.

Este mismo decreto estableció que el Programa ICIC pasara a depender de la Dirección Nacional de Infraestructuras Críticas de la Información y Ciberseguridad, creada dentro del ámbito de la nueva Subsecretaría de Protección de Infraestructuras Críticas de Información y Ciberseguridad.

Así se dispuso que la responsabilidad primaria de la Subsecretaría es la de entender en todos los aspectos relativos a la ciberseguridad y protección de las infraestruc-

turas críticas, comprendiendo la generación de capacidades de detección, defensa, respuesta y recupero ante incidentes del Sector Público Nacional.

Para ello, la Subsecretaría debe llevar adelante acciones similares a las previstas para el Programa ICIC, tales como –por solo mencionar algunas–:

- Entender, asistir y supervisar en los aspectos relativos a la seguridad y privacidad de la información digitalizada y electrónica;
- Elaborar normas y estándares destinados a incrementar los esfuerzos orientados a elevar los umbrales de seguridad en los recursos y sistemas relacionados con las tecnologías informáticas;
- Dictar la Política de Seguridad Modelo de la Información;
- Colaborar con el sector privado para elaborar en conjunto políticas de resguardo de la seguridad digital con actualización constante;
- Establecer prioridades y planes estratégicos para liderar el abordaje de la ciberseguridad, asegurando la implementación de los últimos avances en tecnología para la protección de las infraestructuras críticas.

Asimismo, la Resolución N°1046/15 de Jefatura de Gabinete de Ministros,[23] estableció la creación de tres direcciones y dos coordinaciones dependientes de la Dirección Nacional de Infraestructuras Críticas de Información y Ciberseguridad, cada una a cargo de determinadas acciones, a saber:

1. Dirección de Elaboración e Interpretación Normativa;
2. Dirección Técnica de Infraestructuras Críticas de Información y Ciberseguridad;
3. Dirección de Capacitación, Concientización y Difusión;
4. Coordinación de Procesos y Proyectos;
5. Coordinación de Desarrollo e Investigación.

[23] Resolución N°1046/2015. Disponible en: http://www.infoleg.gob.ar/infolegInternet/anexos/250000-254999/251022/norma.htm

iv Nueva Doctrina de Inteligencia Nacional y la Dirección Operacional de Inteligencia sobre la Ciberseguridad

El 6 de julio de 2015, en forma posterior a la reforma de la ley de Inteligencia –Ley 27.126–, entró en vigencia el Decreto N°1311/15,[24] que estableció la Nueva Doctrina de Inteligencia Nacional como cuerpo doctrinario, la estructura orgánica y funcional del nuevo organismo y un nuevo régimen profesional del personal de la Agencia Federal de Inteligencia (AFI).

El Capítulo I del Anexo I, al desarrollar el marco para la "Inteligencia para la Defensa y Seguridad Democráticas", establece que la inteligencia nacional es una actividad que se inscribe dentro del marco del Estado Constitucional social y democrático de derecho orientada a producir conocimientos acerca de las problemáticas –riesgos, conflictos– inscritas en la defensa nacional y la seguridad interior. La desviación de fines del sistema de inteligencia argentino motivó que se aclare que la inteligencia nacional debe velar por la protección y el cuidado de los argentinos, y no "espiarlos". Por ello el sistema de inteligencia nacional se configura como un "observatorio" abocado exclusivamente a la producción y gestión de conocimientos acerca del conjunto de problemáticas relevantes en materia de defensa nacional y seguridad interior.

Al explicitar las problemáticas que se consideran insertas en el ámbito de Seguridad Interior, refiere que éstas comprenden los fenómenos delictivos violatorios de las libertades y derechos de las personas y del Estado Constitucional social y democrático de derecho, y específicamente aquellos fenómenos delictivos complejos de relevancia federal.

A renglón seguido detalla los fenómenos delictivos complejos de relevancia federal:

1. Terrorismo y sus diferentes manifestaciones globales y/o locales, estatales y no estatales;

[24] Decreto N°1311/2015. Disponible en: http://www.infoleg.gob.ar/infolegInternet/anexos/245000-249999/248914/norma.htm

2. Atentados contra el orden constitucional y la vida democrática, se trate de grupos políticos y/o militares o de grupos económicos y/o financieros.

3. Criminalidad organizada, en particular narcotráfico, trata de personas, delincuencia económica y financiera, tráfico de armas, etc.

4. Acciones que atenten contra la *ciberseguridad*, delitos contra la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, las redes o los datos, o parte de ellos, el uso fraudulento y la difusión ilegal de contenidos. (el resaltado nos pertenece)

En el Capítulo II de la Nueva Doctrina, bajo el título "Dimensiones y Actividades de la Inteligencia Nacional" (Anexo I), se definen los alcances de la producción de inteligencia nacional, que comprende:

- La inteligencia nacional estratégica
- La contrainteligencia
- La inteligencia criminal
- La inteligencia estratégica militar

De las cuatro áreas mencionadas, la ciberseguridad aparece mencionada en el desarrollo de la inteligencia criminal. Así dice que la inteligencia criminal "comprende la producción de inteligencia referida a las problemáticas delictivas y, en particular, a aquellas problemáticas delictivas complejas de relevancia federal relativas al terrorismo, los atentados contra el orden constitucional y la vida democrática, la criminalidad organizada y los atentados contra la ciberseguridad".

A partir del dictado del Decreto 656/16, el Poder Ejecutivo derogó los Anexos II a VII del Decreto 1311/15, es decir, aquellos referidos a la Estructura Orgánica y Funcional de la AFI, su Estructura Organizativa, los Regímenes Profesionales de los Escalafones de Inteligencia, Seguridad y Apoyo, y el Régimen de Administración de Fondos de la AFI.

A pesar de que los anexos mencionados fueron eliminados, consideramos de relevancia mencionar parte del Anexo II, en el cual aparecía el término ciberseguridad,

debido a que el mismo muestra cómo había sido pensado el funcionamiento de esta temática dentro del sistema de inteligencia.

El Anexo II del Decreto 1311/15 contenía la descripción de la "Estructura Orgánica y Funcional de la Agencia Federal de Inteligencia". En su Título II, Capítulo 4, se desarrollaba la estructura operacional de inteligencia de la AFI, dentro de la cual se encuentraban detalladas las funciones y composición de la Dirección Operacional de Inteligencia sobre la Ciberseguridad, que había sido pensada para tener sede en la central de la AFI, en la calle 25 de Mayo 11 de la Ciudad de Buenos Aires.

El objetivo de la Dirección Operacional de Inteligencia sobre la Ciberseguridad era "la producción de inteligencia orientada al conocimiento de las acciones que atenten contra la ciberseguridad en el marco de la defensa nacional o la seguridad interior, y de los grupos nacionales o extranjeros responsables de llevarlas a cabo".

La Dirección Operacional se componía a su vez por dos direcciones:

Dirección de Inteligencia Informática: a cargo de la producción de inteligencia orientada al conocimiento de las actividades relativas a riesgos y conflictos vinculados o derivados del uso de las tecnologías de la información y la comunicación, que afecten la defensa nacional o la seguridad interior, y de los grupos nacionales o extranjeros responsables de llevar a cabo estas actividades.

Dirección de Inteligencia sobre Delitos Informáticos: a cargo de la producción de inteligencia orientada al conocimiento de las actividades que pudieran configurar delitos informáticos en cualquiera de sus formas y modalidades, y de los grupos nacionales o extranjeros responsables de llevar a cabo estas actividades.

El Anexo II establecía que la Dirección Operacional de Inteligencia sobre la Ciberseguridad "desarrolla las actividades institucionales de recolección, gestión y análisis de la información y está integrada por una dotación de oficiales y analistas de inteligencia especializados en ciberseguridad".

Por otra parte, el Decreto 656/16 faculta al nuevo Director de la AFI a aprobar su propia estructura orgánica, así como a dictar normas complementarias y aclaratorias. Uno de los principales problemas que pueden derivarse de ello, es que la creación de una nueva estructura orgánica se dé bajo absoluto secreto, lo que significaría un gran retroceso en el proceso de democratización del sistema de inteligencia, al no conocerse siquiera cómo es la composición interna del organismo.

v Subsecretaría de Tecnología y Ciberseguridad

Con el cambio de administración y la llegada de nuevas autoridades al Estado luego de las elecciones nacionales a finales de 2015, el Poder Ejecutivo tomó una serie de medidas dispuestas a reorganizar parte de la estructura de los distintos ministerios, tomando como modelo la estructura que había armado en la Ciudad Autónoma de Buenos Aires.

Uno de esos cambios cobró vida a través del Decreto N°13/16, que entró en vigencia el 5 de enero de 2016. A partir del mismo se creó el Ministerio de Modernización –en la órbita del Sector Público Nacional–, que modifica el esquema de organismos que veníamos describiendo hasta este momento.[25]

El Ministerio de Modernización cuenta con cuatro secretarías: Secretaría de Empleo Público, Secretaría País Digital, Secretaría de Gestión e Innovación Pública, y Secretaría de Modernización Administrativa, cada una con sus correspondientes subsecretarías. Por otra parte, cuenta a su vez con cuatro subsecretarías que dependen directamente del Ministro: Subsecretaría de Coordinación Administrativa, Subsecretaría de Relaciones Laborales y Fortalecimiento del Servicio Civil, Subsecretaría de Tecnología y Ciberseguridad, y Subsecretaría de Telecomunicaciones y Redes Públicas.

A los fines de este documento nos centraremos entonces en la Subsecretaría de Tecnología y Ciberseguridad. Esta subsecretaría es la que pasa a nuclear gran parte de las distintas dependencias que hemos ido desarrollando en esta sección,

[25] Decreto N°13/2016. Disponible en: http://www.infoleg.gob.ar/infolegInternet/anexos/255000-259999/257556/texact.htm

por ende, se convierte en la pata central en lo que hace a la ciberseguridad en Argentina.

La Subsecretaría de Tecnología y Ciberseguridad está a cargo de:[26]

1. **Oficina Nacional de Tecnologías de Información (ONTI)**: La cual tiene como principal objetivo intervenir en la formulación de políticas e implementación del proceso de desarrollo e innovación tecnológica para la transformación y modernización del Estado, promoviendo la integración de nuevas tecnologías, su compatibilidad e interoperabilidad de acuerdo con los objetivos y estrategias definidas en el Plan de Modernización del Estado.[27]

2. **Dirección Nacional de Infraestructura Tecnológica y Operaciones**: Deberá intervenir en los aspectos relativos al desarrollo y mantenimiento de la infraestructura tecnológica, como así también en la administración y procesamiento informático de sistemas y datos críticos, en el ámbito de la Administración Pública Nacional.

3. **Dirección Nacional de Infraestructuras Críticas de Información y Ciberseguridad**: Asistirá en todos los aspectos relativos a la ciberseguridad y protección de las infraestructuras críticas, comprendiendo la generación de capacidades de detección, defensa, respuesta y recupero ante incidentes del Sector Público Nacional.

De esta manera, se traslada la estructura de las dependencias encargadas de la ciberseguridad nacional de la órbita de la Jefatura de Gabinete de Ministros a una Subsecretaría dentro del Ministerio de Modernización.

El Decreto N°13/16 asigna también los objetivos de la Subsecretaría, entre los cuales encontramos –solo por nombrar algunos–:

[26] Decisión Administrativa 232/2016, Ministerio de Modernización. Disponible en: http://www.infoleg.gob.ar/infolegInternet/anexos/255000-259999/259845/norma.htm

[27] Plan de Modernización del Estado, Ministerio de Modernización. Decreto 434/2016, marzo 2016. Disponible en: http://www.infoleg.gob.ar/infolegInternet/anexos/255000-259999/259082/norma.htm

- Entender en la elaboración de la estrategia nacional de Infraestructura tecnológica, la protección de infraestructuras críticas de información y ciberseguridad, a nivel nacional.
- Dirigir y operar centros de datos y cómputos, a efectos de brindar servicios centrales de infraestructura a otras jurisdicciones, optimizando el uso de los recursos, mejorando la seguridad y aumentando los niveles de calidad en la prestación del servicio.
- Entender en materia de dictado de normas, políticas, estándares y procedimientos de Tecnología y Seguridad Informática en el ámbito de su competencia.
- Asistir al Ministro en la formulación de un marco regulatorio específico que propicie la identificación y protección de las infraestructuras críticas del Sector Público Nacional, y a las organizaciones civiles, del sector privado y del ámbito académico que así lo requieran, fomentando la cooperación y colaboración de los mencionados sectores.
- Entender en los procesos relativos al accionar del equipo de respuesta a emergencias informáticas a nivel nacional (CERT Nacional).
- Dirigir y supervisar el accionar de la Oficina Nacional de Tecnologías de Información (ONTI).

vi Subsecretaría de Ciberdefensa

El 7 de enero de 2016, mediante el Decreto N°42/16, se crea en el ámbito de la Secretaría de Ciencia, Tecnología y Producción para la Defensa –dentro del Ministerio de Defensa–, la Subsecretaría de Ciberdefensa.[28]

Dentro de los objetivos planteados por el Decreto para la Secretaría de Ciencia, Tecnología y Producción para la Defensa se encuentran:

[28] Decreto N°42/2016. Disponible en: http://www.infoleg.gob.ar/infolegInternet/anexos/255000-259999/257609/norma.htm

- Entender en la formulación, aprobación y supervisión del cumplimiento de las políticas y programas de los organismos de investigación y desarrollo del sector de Ciberdefensa.
- Entender en la coordinación y conducción superior de los organismos científicos y tecnológicos del área Ciberdefensa.
- Entender en el impulso y promoción del intercambio de formación técnica relacionada con la Ciberdefensa a nivel extrajurisdiccional.

Por otra parte, la Subsecretaría de Ciberdefensa tiene como principales acciones (el resaltado nos pertenece):

- Asistir al Secretario de Ciencia, Tecnología y Producción para la Defensa en el planeamiento, diseño y elaboración de la política de ciberdefensa de acuerdo a lo establecido en el Ciclo de Planeamiento de la Defensa Nacional en coordinación con la Subsecretaría de Planeamiento Estratégico y Política Militar.
- Entender en la *coordinación con los organismos y autoridades de los distintos Poderes del Estado para contribuir desde la Jurisdicción a la política nacional de ciberseguridad y de protección de infraestructura crítica*.
- Ejercer el control funcional sobre el Comando Conjunto de Ciberdefensa,[29] del Estado Mayor Conjunto de las Fuerzas Armadas.
- Intervenir en el diseño de políticas, normas y procedimientos destinados a garantizar la seguridad de la información y a coordinar e integrar los centros de respuesta ante emergencias teleinformáticas.

vii De la normativa a la práctica: el estado de situación real de la ciberseguridad en la Argentina

Hasta este punto hemos analizado qué es lo que establecen las principales normas que directa o indirectamente están vinculadas a la ciberseguridad en el país. A lo

[29] Sitio web oficial: http://www.fuerzas-armadas.mil.ar/Dependencias-CIBDEF.aspx

largo de esta investigación y a través de distintas fuentes expertas entrevistadas en el proceso, pudimos comprender cómo las mismas se traducían a la realidad, qué se cumplió y qué no, qué tan efectivas fueron y qué debería haberse planteado distinto.

"Si bien considero que las Misiones y Funciones del programa [ICIC] son apropiadas, creo que su ejecución ha sido deficiente.", comenta el especialista Mariano del Rio,[30] "Al día de hoy, no contamos con un catálogo de las infraestructuras críticas, tampoco con una estrategia nacional de ciberseguridad. Sí se han realizado numerosos eventos. Respecto al impacto del programa en políticas públicas, creo que debido a la ausencia de una visión integral de la ciberseguridad, que generalmente se lleva a cabo a través de una estrategia nacional de ciberseguridad, no veo que se haya logrado influir a otros estratos del Estado con dicho programa".

Con la información pública disponible y verificable a la que se pueda acceder, si volvemos a leer detenidamente los objetivos asignados al ICIC, la primera conclusión a la que uno arriba es que un gran porcentaje de los mismos fue cumplido parcialmente o directamente nunca se cumplió. A lo largo del trabajo de investigación se intentó en varias oportunidades contactar con los funcionarios a cargo de las distintas dependencias del Estado responsables de la ciberseguridad del país para poder acceder a mayores precisiones sobre el estado de situación, sin lograr respuesta alguna.

Como determina el experto Iván Arce,[31] uno de los principales problemas fue

[30] Entrevista a Mariano M. del Rio, abril 2016. Es especialista en Ciberseguridad, Compliance y Privacidad con más de 10 años de experiencia en la implementación de Programas de Seguridad de la Información y cumplimiento de las principales leyes y regulaciones en la materia en diferentes industrias. Fundador de SecureTech, empresa argentina de servicios de ciberseguridad y compliance.

[31] Entrevista con Iván Arce, mayo 2016. Es Director del Programa de Seguridad en TIC (STIC) de la Fundación Dr. Manuel Sadosky, una entidad sin fines de lucro publico-privada dedicada a promover y robustecer en todo lo referente a Tecnologías de la Información y Comunicación (TIC) la articulación entre el sistema científico-tecnológico y el sector productivo de la Argentina. Entre 1996 y 2012 ocupó múltiples roles en Core Security Technologies, una empresa que fundó con 4 amigos en Buenos Aires. Es miembro fundador del Center for Secure Design de la sociedad de computación del IEEE, editor de la revista IEEE Security and Privacy durante el período 2002-2015 y orador frecuente en congresos y conferencias de seguridad informática.

que "Al ICIC se le dan una serie de responsabilidades y atribuciones que son inmensas, no solamente para su estructura sino para su diseño institucional. No quedó bien en claro qué es lo que querían hacer, cuáles eran las políticas y cuáles eran los objetivos. Lo que sí se logró fue la redacción de una política modelo de seguridad informática, que es una adaptación de la ISO 27001 para que adopten todos los organismos del Estado. La adopción no es obligatoria sino voluntaria, al igual que como en el Programa ICIC, que también era voluntaria. [La normativa planteaba] toda una serie de cosas que en los papeles podrían ser interesantes, pero que en la práctica la ejecución –que yo sepa– no ha sido buena".

"Los esfuerzos que hubo en los últimos años, desde el punto de vista institucional son un paso en la dirección correcta, pero aún falta, falta estructurar eso en una estrategia nacional, cubrir los agujeros y los baches conceptuales, delimitar y agregar lo faltante. [La ciberseguridad] no es un tema sólo de seguridad, defensa e inteligencia, son varias cosas más, aspectos económicos, sociales y comerciales. Faltan cuestiones regulatorias, cuestiones de desarrollo tecnológico, de tener un ecosistema sustentable de ciberseguridad. Hay que pensarlo en forma holística", concluye Arce.

Para el Dr. Hugo Scolnik,[32] "Es fundamental tener un centro unificado que coordine a todos los organismos descentralizados que se ocupen de las distintas estructuras del Estado. Debe haber un intercambio de experiencias entre los funcionarios y empleados de las distintas dependencias, todos los ministerios deberían estar coordinados".

Los expertos consultados coinciden en que la Jefatura de Gabinete era el lugar adecuado para ubicar la temática de la ciberseguridad, principalmente porque desde ahí se puede llegar a todos los estratos del Estado con mayor eficacia y hay un vínculo directo con la Presidencia; esto es fundamental debido a la mirada holística y transversal que necesariamente debe tener el desarrollo de las políticas de ciberseguridad.

[32] Entrevista con el Dr. Hugo Scolnik, mayo 2016. Es Lic. en Matemática por la Universidad de Buenos Aires y Doctor en Matemática por la Universidad de Zurich. Es profesor consulto titular del Departamento de Computación de la FCEN-UBA y CEO de la empresa Firmas Digitales SRL. Desde el 2009 se desempeña como Director Adjunto de la Maestría en Seguridad Informática de la Universidad de Buenos Aires.

El paso al Ministerio de Modernización, realizado a fines de 2015, puede ser determinante en la efectiva implementación de las políticas nacionales si no se pone especial atención en cómo las mismas serán implementadas y llevadas a la práctica. En este sentido, si bien el campo de acción puede resultar acotado –jerárquicamente, al ser una subsecretaría dentro de uno de los tantos ministerios–, todo dependerá de cómo se plantea el trabajo a futuro, y fundamentalmente cómo se pretende impulsar a nivel nacional que la estrategia de ciberseguridad sea respetada y seguida por todos los estratos del Estado, así como del sector privado.

La problemática de la ciberseguridad también plantea cuestiones que deben ser abordadas desde la protección de los datos personales. El ordenamiento jurídico argentino establece altos estándares de protección a la privacidad y la ley 25.326 –de protección de datos personales– sigue el modelo de la legislación europea. En este sentido, la prohibición de procesar y transferir datos personales sin el consentimiento del titular de los datos se vuelve uno de los pilares de nuestro sistema. Sin embargo, dicha regla no se aplica cuando se trata de bases de datos de organismos estatales. La amplia redacción de la norma permite que distintos organismos estatales puedan tratar datos personales más allá de lo que es estrictamente necesario y proporcional.[33]

De esta manera, las autoridades cuentan con un gran margen de discrecionalidad, sin que haya un adecuado control de órganos independientes. Así, los ciudadanos se ven privados de numerosas herramientas para protegerse frente a eventuales invasiones a su privacidad. Debido a su falta de independencia funcional y los problemas presupuestarios producto de la ausencia de autarquía financiera, la Dirección Nacional de Protección de Datos Personales (DNPDP) no ha podido llevar a cabo con eficiencia su labor de contralor, adoptando desde su creación un papel más orientado hacia la educación, participación y difusión, que de fiscalización del cumplimiento de la ley.

[33] El Estado recolector, ADC, septiembre 2014. Disponible en: https://adcdigital.org.ar/portfolio/el-estado-recolector/

viii Una mirada exterior a la ciberseguridad en la Argentina, con la que no estamos necesariamente de acuerdo

a "Seguridad Cibernética e Infraestructura Crítica en las Américas"

A comienzos de 2015, la OEA junto a Trend Micro Inc. presentaron el informe "Seguridad Cibernética e Infraestructura Crítica en las Américas". Mencionaremos los descubrimientos a los que arribaron para el caso particular de la Argentina.

El reporte de Trend menciona que hasta el año 2014, el ICIC había logrado (Pág. 41):

- Ayudar a la aprobación de legislación relacionada con el cibercrimen; "lo que ha permitido la investigación y persecución exitosas de varios casos de criminales cibernéticos", pero no menciona más detalles sobre qué casos puntuales se vieron beneficiados o estadísticas que permitan ponderar el éxito de la legislación, por ejemplo.
- Desarrollar la iniciativa "Internet Sano", creada con el objetivo de promover y facilitar material educativo sobre el uso responsable de las tecnologías de información y comunicaciones e Internet.
- Llevar a cabo ejercicios de respuesta a incidentes informáticos (denominados ENRIC), que habían comenzado a tener lugar desde el año 2012.

Por otra parte, establece también que "El ICIC ha tenido una participación activa en los eventos patrocinados por la Organización de los Estados Americanos (OEA), el Instituto de Estudios de Seguridad de la Unión Europea (UEISS), la Agencia Internacional de Energía Atómica (IAEA), Meridian Process, entre otros" (Pág. 42).

Finalmente, el reporte concluye la sección sobre Argentina compartiendo tres puntos centrales que fueron determinados en el informe "Tendencias de Seguridad Cibernética en América Latina y el Caribe"[34] –producido por la OEA y Syman-

[34] Tendencias de Seguridad Cibernética en América Latina y el Caribe, OEA, Symantec, página 38. Junio 2014. Disponible en: https://www.symantec.com/es/mx/page.jsp?id=cybersecurity-trends

tec–; los mismos fueron identificados por las autoridades gubernamentales de Argentina como impedimentos principales a sus iniciativas en curso relacionadas con la seguridad y los delitos cibernéticos, estos son:

- Falta constante de concientización entre las partes interesadas en todos los niveles;
- Problemas y cuestiones relacionados con la privacidad;
- Financiación insuficiente.

b "Ciberseguridad: ¿Estamos preparados en América Latina y el Caribe?"

En marzo de 2016, el BID y la OEA publicaron el informe "Ciberseguridad 2016: ¿Estamos preparados en América Latina y el Caribe?",[35] en el cual se analizó el nivel de madurez de los distintos países de la región en torno a cuatro puntos de vista de la seguridad cibernética: Política y Estrategia, Cultura y Sociedad, Educación, Marcos legales, y Tecnologías.

En los perfiles de los países, para el caso de la Argentina, el BID establece que "bajo la dirección del Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad (ICIC) y en coordinación con diversos organismos, instituciones académicas y el sector privado, el Gobierno de Argentina ha desarrollado un proyecto de Estrategia Nacional de Seguridad Cibernética que se encuentra en espera de adopción". A lo largo de la investigación llevada a cabo para el presente informe, no nos hemos topado con indicios que den lugar a suponer la existencia de un proyecto de una estrategia nacional de ciberseguridad, mucho menos para suponer que la misma se encontraría en el proceso final de implementación. Diversos expertos técnicos entrevistados coincidieron en que una de las falencias del ICIC era la falta de publicación de materiales vinculados con sus objetivos y su trabajo, y que sirviese a los fines de que diversos actores de la sociedad pudiesen colaborar en perfeccionar las políticas de ciberseguridad; por

[35] Ciberseguridad 2016, BID. Marzo 2016. Disponible en: http://observatoriociberseguridad.com/graph/countries//selected//0/dimensions/1-2-3-4-5

ejemplo, una de las obligaciones del ICIC era la publicación de informes anuales; desde su concepción, el ICIC no ha publicado ni un solo informe.

En tal sentido, si evaluamos el trabajo del ICIC desde su creación en base a la publicación de materiales (entiéndase: informes, políticas, estrategias, etcétera) que responden a sus funciones determinadas por la normativa, podríamos afirmar que nunca existieron informes anuales, ni mucho menos un proyecto de estrategia nacional. A lo largo de la investigación se insistió para conseguir una entrevista con las autoridades responsables de ICIC en el año 2015 –sin suerte alguna–, con el fin de poder conocer la versión oficial sobre el trabajo desarrollado por ICIC.

La falta de publicidad y transparencia en el trabajo del ICIC, sumado a la falta de participación de los diversos actores que deberían haber sido convocados por el ICIC para acompañar en el proceso de elaboración de políticas de ciberseguridad (comunidad técnica, academia, sociedad civil, sector privado), da cuenta de dos errores fundamentales en el trabajo de confección de políticas públicas que, como hemos visto, es remarcado consistentemente en estudios internacionales.

El BID destaca también la expansión de los servicios de gobierno electrónico y de comercio electrónico en el país, respecto a los cuales remarca que "las entidades gubernamentales han liderado campañas de concientización para educar al público sobre la seguridad cibernética", en referencia a iniciativas como "Internet Sano", de ICIC, y "Con Vos en la Web", iniciativa de la Dirección Nacional de Protección de Datos Personales (bajo la órbita del Ministerio de Justicia y Derechos Humanos). Ambas iniciativas fueron muy bien recibidas por múltiples sectores de la sociedad y elogiadas por comenzar a transitar el camino en la dirección correcta hacia una mayor capitación en temas de tecnología y derechos, fundamentalmente en las demografías más vulnerables, como son los niños, niñas y adolescentes. Los proyectos cuentan con materiales enfocados tanto para padres como para jóvenes, con guias sobre temas como cyberbullying, grooming,[36] amenazas en Internet, y consejos sobre cómo proteger tu intimidad, reputación e imagen en Internet. Actualmente, ambas iniciativas se encuentran cerradas y ninguno de los respectivos organismos ha comunicado planes sobre su

[36] Grooming: creación de lazos de amistad abusivos en la web con los niños para atraerlos al abuso sexual o la trata de personas.

continuidad. Ante esta situación, es dable destacar la labor de la Unidad Fiscal Especializada en Ciberdelincuencia (UFECI) del Ministerio Público Fiscal en buscar aportar a la concientización del uso de Internet a través de la elaboración de material didáctico, como su guía "¿Cómo evitar ser una víctima en las redes sociales?".[37]

Para cerrar este capítulo, cabe mencionar que la información plasmada en informes como los publicados por Trend y Symantec, debe ser tomada en consideración respecto del papel que juegan estas empresas en el mercado global de la seguridad digital, pues su fin comercial es el desarrollo de software de seguridad, por lo que las estadísticas pueden no representar una mirada integral del estado de situación de un país, sino más bien sesgada debido al tipo de información a la que estas firmas privadas tienen acceso o recopilan, y que es analizada acorde a sus propios intereses. Si no se dan a conocer detalladamente las metodologías de estudio utilizadas en informes, las políticas de ciberseguridad de un país no pueden ser definidas en base a estudios elaborados por empresas que tienen intereses en el mercado; por lo que se convierte en un pilar fundamental la elaboración de investigaciones y estudios propios de quienes formen parte del proceso de confección de políticas de ciberseguridad, contando con la asistencia de consultores externos de la sociedad como expertos de la comunidad técnica y académica.

VI Inteligencia y ciberseguridad

i El vínculo de la inteligencia con la ciberseguridad

Como bien hemos analizado previamente, una de las tendencias a nivel global en el discurso de la ciberseguridad está dirigida a afrontar esta práctica con miras a proteger a la sociedad como un conjunto, y no a individuos específicos, todos los estratos del Estado y del ámbito privado deben trabajar en forma holística. Esto lleva a que la soberanía nacional forme parte de la política de ciberseguridad, lo

[37] ¿Cómo evitar ser una víctima en redes sociales?, UFECI, MPF. Abril 2016. Disponible en: http://www.fiscales.gob.ar/procuracion-general/como-evitar-ser-una-victima-en-las-redes-sociales/

cual abre la puerta a que los encargados de la inteligencia y la defensa nacional formen parte de la discusión, elaboración y puesta en práctica de dichas políticas.

La Nueva Doctrina de Inteligencia Nacional identifica a la ciberseguridad como un nuevo fenómeno delictivo complejo, que deberá enfrentar la Agencia Federal de Inteligencia a través de la producción de inteligencia nacional, específicamente de inteligencia criminal. Si bien la estructura orgánica que se había creado para la AFI, que incluía la Dirección Operacional de Inteligencia sobre Ciberseguridad, fue derogada, cabe mencionar las explicaciones dadas por el entonces Director de la Agencia, Oscar Parrilli, para comprender cómo había sido pensada a la ciberseguridad dentro del sistema de inteligencia nacional.

Durante una conferencia de prensa brindada en julio de 2015 para presentar la Nueva Doctrina de Inteligencia Nacional, Parrilli informó que la Dirección Operacional estaría encargada de "todo lo que en el mundo moderno hoy son los delitos cibernéticos, informáticos, todo lo que es la infraestructura crítica de la Argentina, que pasa por sus centrales nucleares, bancos y demás y toda la protección que se tiene que llevar adelante. En este sentido han ocurrido en los últimos tiempos noticias muy impactantes, ha sido amenazado y hackeado el parlamento alemán, han sido hackeadas instituciones de Estados Unidos, de Inglaterra, y aquí en la Argentina no teníamos una política que previera, estudiara, analizara y realizara inteligencia sobre estos temas. La hemos creado, la vamos a poner en marcha en los próximos días, y además fundamentalmente también tenemos el orgullo de decir que va a estar al frente de este organismo un ingeniero informático argentino muy prestigiado, que viene de la actividad privada, que conoce profundamente todos estos temas y que nos va a dar una gran ayuda a todos los argentinos para evitar este tipo de amenazas y acciones que pueden afectar a la seguridad y la defensa nacional".[38]

Dado el breve período de tiempo que estuvo en funcionamiento la Dirección Operacional de Inteligencia sobre la Ciberseguridad, no es demasiada la información que hemos podido obtener en relación a la misma, sólo aquella surgida de algu-

[38] Parrilli, Oscar. Conferencia de prensa. Casa de Gobierno. 7 de julio de 2015. Disponible en: http://www.casarosada.gob.ar/informacion/conferencias/28837-conferencia-del-titular-de-la-afi-oscar-parrilli-en-casa-de-gobierno

nas notas informativas. En una entrevista publicada el 1 de diciembre de 2015, Parrilli informó que la Dirección estaba funcionando en plena capacidad hacía poco menos de un mes y que su actividad consistía en mirar los ciberataques que suceden en el mundo, analizar en qué situación el país se podría considerar amenazado y realizar las advertencias adecuadas en los casos que sean necesarios; además de intervenir en investigaciones judiciales si la Justicia Federal lo requiere.[39]

Fuentes cercanas al ex Director de la AFI mencionaron que la elección del término "ciberseguridad" no responde más que a un simple impulso novedoso, sin tener realmente en consideración las implicancias del uso de este término en el ámbito de la inteligencia nacional, más allá de las advertencias realizadas por expertos en la materia desde su círculo profesional.

Es ante este escenario en el cual la falta de una definición de ciberseguridad adoptada a nivel nacional trae inconvenientes. El no tener delimitado precisamente qué es y que no es ciberseguridad, se deja abierta la puerta a que se tomen ciertas libertades en su interpretación.

Los especialistas y expertos en ciberseguridad consultados a lo largo de este proyecto parecen coincidir en que la ciberseguridad requiere de una actividad de inteligencia, vinculándolo con la defensa nacional y la protección de los ciudadanos. Mariano del Rio sostiene que "basta con revisar las limitaciones que tienen las fuerzas de seguridad para abordar la temática de la ciberseguridad. Lamentablemente la AFI ha sido utilizada para otros fines que nada tienen que ver con brindar información de valor para combatir el crimen organizado. Hoy en día, la información que pueda surgir respecto a temáticas de ciberseguridad, es de valor para la investigación y combate de todo tipo de actividad ilícita".

La nueva estructura orgánica que adopte la AFI deberá tener en consideración sus límites de actuación en este tipo de temáticas. Por ejemplo, bajo la antigua estructura, podíamos encontrar que una de las tareas de la Dirección de Inteligencia sobre Delitos Informáticos –dentro de la Dirección Operacional sobre Ciberseguridad–, era la "producción de inteligencia orientada al conocimiento de

[39] Bullentini, Ailín. "Predecir y prevenir ciberataques", Página/12, 1 de diciembre de 2015. Disponible en: http://www.pagina12.com.ar/diario/elpais/1-287308-2015-12-01.html

las actividades que pudieran configurar delitos informáticos en cualquiera de sus formas y modalidades". ¿Ello implicaría entonces convertir a la AFI en una suerte de policía cibernética, con facultades de investigación sobre la vida online de los ciudadanos? ¿Qué aporte diferenciador podría en ese caso lograr la AFI que no sea ya logrado por la Unidad Fiscal Especializada en Ciberdelincuencia (UFECI)[40] a cargo de la Procuración General de la Nación?

ii Breve historia de la inteligencia en democracia, un sistema al que le cuesta abandonar sus vicios

Los servicios de inteligencia en la Argentina surgen a partir de la Segunda Guerra Mundial, como una tendencia global con el afán de defender la Nación y sus intereses. Durante años fueron regulados por decretos secretos del Poder Ejecutivo, hasta que en el año 2001 se sanciona la Ley de Inteligencia Nacional (N°25.520) con el fin de definir las actividades de inteligencia, delimitar los campos de acción e imponer mecanismos de control. Intento fútil que no logró modificar el funcionamiento de un órgano que mantenía prácticas, personal y costumbres arrastradas desde la época de la dictadura militar. Esto es esencial para entender por qué el principal organismo de inteligencia de la Argentina se mantuvo alejado del proceso de democratización iniciado en 1983, la agencia de inteligencia estuvo estrechamente vinculada a las dictaduras que gobernaron la Argentina durante las décadas del 50 y del 70, así como también con los crímenes de lesa humanidad cometidos durante aquellos años.

Como ya ha expuesto la ADC previamente en su informe "El (des) control democrático de los organismos de inteligencia en Argentina",[41] con el regreso de la democracia la agencia de inteligencia se vió envuelta en constantes reformas, presidencia tras presidencia, que respondían más a una cuestión de poder

[40] Di Nicola, Gabriel. "Crean una fiscalía especializada para la lucha contra el cibercrimen", La Nación, 18 de noviembre de 2015. Disponible en: http://www.lanacion.com.ar/1846626-crean-una-fiscalia-especializada-para-la-lucha-contra-el-cibercrimen

[41] El (des) control democrático de los organismos de inteligencia en Argentina, ADC, 2015. Disponible en: https://adcdigital.org.ar/portfolio/des-control-democratico-los-organismos-inteligencia-argentina/

político, que de buscar realmente democratizar un órgano que seguía siendo usado como carta blanca por quien ostentara el cargo de Presidente, haciéndose uso del aparato de inteligencia del Estado con fines de espionaje político (a funcionarios, opositores, sindicatos, periodistas, entre otros), para financiar sobornos a jueves y fiscales mediante el uso de fondos reservados del organismo, obstaculizar la investigación de uno de los casos más polémicos de la historia Argentina vinculados con terrorismo, disputas con las fuerzas de seguridad como la Policía Federal Argentina, y la represión de los movimientos sociales ante la crisis económica en el año 2001.

Estos son algunos de los sucesos que han tenido a la agencia de inteligencia como eje central de la historia. Como se concluyó en mencionado informe, la falta de consecuencias a partir de los escándalos que involucraron al sistema de inteligencia encuentra su razón de ser en el vínculo estrecho de los organismos de inteligencia con un poder ejecutivo que sostiene parte de su poder sobre un organismo secreto, con acceso a vastos recursos económicos y alejado de controles democráticos.

En el informe "Quien vigila a quienes vigilan" (ADC, 2014),[42] realizamos un estudio comparativo sobre distintos sistemas de control de los organismos de inteligencia especialmente en América Latina. En el caso de la Argentina, quien toma este rol es la Comisión Bicameral de Fiscalización de los Órganos y Actividades de Inteligencia (en el Congreso de la Nación), creada en el año 2001 con la sanción de la ley de inteligencia. En dicho estudio se determinó que la Comisión no comenzó a funcionar sino hasta 3 años después de su creación, que la misma mantiene un riguroso secreto sobre sus actividades, sin informar siquiera sobre sus reuniones, informes o agenda de trabajo, que incluso varios miembros de la Comisión nunca habían recibido el informe anual que la Comisión debía elaborar anualmente por ley para elevar al Congreso y al Poder Ejecutivo.

[42] Quién vigila a quienes vigilan, ADC, 2014. Disponible en: https://adcdigital.org.ar/portfolio/quien-vigila-quienes-vigilan/

iii La Agencia Federal de Inteligencia

A fines de 2014, la agencia de inteligencia comenzó uno de sus más polémicos períodos de transición reformativa, que inició con varias internas[43] y el desplazamiento de una de las figuras más controvertidas para la historia de este organismo, el espía Antonio Jaime Stiuso, vinculado –entre otras cuestiones– con la investigación por el atentado a la AMIA, en donde el organismo estuvo involucrado desde el primer momento. Por decisión de la ex Presidente Cristina Fernández de Kirchner, el ex titular de la entonces Secretaría de Inteligencia –Oscar Parrilli– aceptó la renuncia de Stiuso, quien se desempeñó en la AFI como director general de operaciones, y llevaba 43 años como personal de inteligencia.[44] En enero de 2015, el día anterior a declarar en el Congreso por una denuncia que involucraba a las más altas esferas del poder (incluyendo a la ex Presidente Cristina Fernández de Kirchner), apareció muerto de un tiro en la cabeza el fiscal federal a cargo de la causa AMIA, Alberto Nisman.[45]

Esta serie de sucesos, sumado al clima político, llevó a que en marzo de 2015 se sancionara la ley 27.126, la cual introduce una reforma a la ley 25.520 y presenta dos modificaciones importantes a nivel institucional: la creación de la Agencia Federal de Inteligencia (en reemplazo de la ex Secretaría de Inteligencia) y del Departamento de Interceptación y Captación de las Comunicaciones (en reemplazo de la ex Dirección de Observaciones Judiciales).

Posteriormente, con la publicación del Decreto 1311/2015 (y la subsiguiente modificación con el Decreto 2415/2015), se aprueba la Nueva Doctrina de Inteligencia Nacional con el objetivo de determinar la estructura orgánica y funcional de la AFI, así como el régimen profesional del personal de inteligencia.

[43] "Tras una nota de Noticias, cae la cúpula de la SIDE", Perfil, 16 de diciembre de 2014. Disponible en: http://www.perfil.com/politica/Tras-una-nota-de-Noticias-cae-la-cupula-de-la-SIDE-20141216-0039.html

[44] Obarrio, Mariano. "Desplazaron a Stiusso de la Secretaría de Inteligencia", La Nación, 20 de diciembre de 2014. Disponible en: http://www.lanacion.com.ar/1754189-desplazaron-a-stiusso-de-la-secretaria-de-inteligencia

[45] "La interna de la ex SIDE, protagonista en el caso Nisman", Diario Popular, 22 de enero de 2015. Disponible en: http://www.diariopopular.com.ar/notas/214977-la-interna-la-ex-side-protagonista-el-caso-nisman

Un análisis sobre la formación y capacitación del personal de inteligencia puede leerse en el informe "Educar para Vigilar" (ADC, 2015).[46]

Con la creación del Departamento de Interceptación y Captación de las Comunicaciones (DICOM), a cargo de la fiscal Cristina Caamaño, el cual formaba parte de la Dirección General de Investigaciones y Apoyo Tecnológico a la Investigación Penal (DATIP) bajo la órbita del Ministerio Público Fiscal,[47] se buscaba darle mayor independencia a los funcionarios a cargo del trabajo de las interceptaciones, sacándolas del dominio de la agencia de inteligencia, que históricamente había ostentado el poder y monopolio sobre las escuchas telefónicas de la Argentina.

De esta manera, a través del artículo 17 de la ley 27.126, el DICOM se convertía en "el único órgano del Estado encargado de ejecutar las interceptaciones o captaciones de cualquier tipo autorizadas u ordenadas por la autoridad judicial competente".[48] Esto implicó que tanto la AFI, las fuerzas federales (Policía Federal Argentina, Gendarmería, Prefectura, Policía de Seguridad Aeroportuaria), Policía Metropolitana y las policías provinciales, en el caso de necesitar intervenir una línea telefónica o cualquier otro tipo de comunicación de un usuario, deben formalizar su pedido judicialmente, para ser luego procesado por DICOM, por lo que cualquier otra vía utilizada es ilícita. Una explicación más detallada sobre la creación del DICOM y la transición desde la AFI, puede encontrarse en el informe "Educar para vigilar" (ADC, 2015).

A partir de la llegada de la nueva administración al Estado Nacional, con Mauricio Macri encabezando el Poder Ejecutivo, llegaron nuevos vientos de cambio a la inteligencia nacional y la interceptación de comunicaciones.

A comienzos de 2016 fueron designados en la AFI Gustavo Arribas y Silvia Majdalani, como Director y Subdirectora, respectivamente.[49] Lo que motivó a que

[46] Educar para vigilar, ADC, 2015. Disponible en: https://adcdigital.org.ar/portfolio/educar-para-vigilar/

[47] Procuración General de la Nación. Resolución N°2067/15. 7 de julio de 2015. Disponible en (PDF): http://www.fiscales.gob.ar/procuracion-general/wp-content/uploads/sites/9/2015/07/PGN-2067-2015-001.pdf

[48] Artículo 17, Ley 27.126 disponible en: http://www.infoleg.gob.ar/infolegInternet/anexos/240000-244999/243821/norma.htm

[49] Savoia, Claudio. "La interna de la ex Side arde con las designa-

desde la Iniciativa Ciudadana para el Control del Sistema de Inteligencia –del cual la ADC forma parte– se realizara un llamado de atención sobre la situación,[50] debido a que los funcionarios nombrados carecen de formación y conocimientos sobre el funcionamiento del sistema de inteligencia, lo que pone en duda su idoneidad profesional para desempeñar cargos tan delicados.

Por otra parte, a través del Decreto 256/2015, el Poder Ejecutivo transfirió al DICOM de la órbita de la PGN al Poder Judicial bajo la Corte Suprema de Justicia de la Nación (CSJN). A tal fin, mediante la acordada 2/2016, la CSJN creó la Dirección de Captación de Comunicaciones (DCC), que reemplazó en su totalidad al DICOM; situación que ha sido analizada por la ADC.[51]

Los distintos sucesos narrados en este capítulo dan cuenta de las características y los vicios que ha ido desarrollando el sistema de inteligencia en la Argentina, específicamente su agencia central –AFI–, a lo largo de su truculenta historia. Debido al papel que pretende jugar la inteligencia en el desarrollo de las políticas de ciberseguridad, su rol no puede dejarse librado a supuestos y ambigüedades de la letra normativa, por el contrario, para que sus vicios y defectos no impacten de lleno en las políticas de ciberseguridad, es elemental demarcar su campo de acción y cómo formará parte de las mismas.

VII Comentarios finales

Al momento de cierre del presente informe, quedamos al pendiente de la solicitud de entrevistas con las nuevas autoridades responsables de la Subsecretaría de Tecnología y Ciberseguridad, del Ministerio de Modernización; de la Subsecretaría de Ciberdefensa, del Ministerio de Defensa; y del Comando Conjunto de

ciones polémicas", Clarín, 19 de diciembre de 2015. Disponible en: http://www.clarin.com/politica/Agencia_federal_de_Inteligencia_0_1489051101.html

[50] "ICCSI: Problemas en la designación de autoridades de la AFI", 30 de marzo de 2016. Disponible en: https://adcdigital.org.ar/2016/03/30/iccsi-problemas-designacion-autoridades-afi/

[51] "Reflexiones sobre la creación de la Dirección de Captación de Comunicaciones", ADC, 19 de febrero de 2016. Disponible en: https://adcdigital.org.ar/2016/02/19/reflexiones-sobre-la-creacion-de-la-direccion-de-captacion-de-comunicaciones/

Ciberdefensa, del Estado Mayor Conjunto de las Fuerzas Armadas.

VIII Conclusiones

Las iniciativas de los últimos años en el campo de la ciberseguridad, mostraron un paso en la dirección correcta al buscar focalizar el trabajo de esta temática desde el Estado, estableciendo objetivos y tareas que resultaban adecuados para comenzar a desarrollar una verdadera agenda de ciberseguridad que pudiera expandirse a nivel nacional. Como describimos en su pertinente capítulo, en la realidad esta situación no se concretó, no solo debido a la falta de presupuesto correspondiente a los organismos encargados de llevar a cabo estas tareas, sino también a la forma en que los responsables optaron por trabajar la temática, fundamentalmente no trabajando desde la transparencia de sus tareas, acciones y resultados, ni en forma abierta, alentando la participación de expertos en la temática que pudieran aportar su visión, conocimiento y experiencia para mejorar las políticas llevadas a cabo desde el Estado.

Ante la falta de consensos internacionales en cuanto a las definiciones y límites de la ciberseguridad, América Latina aún tiene la oportunidad de avanzar hacia un nuevo concepto de ciberseguridad que no se derive exclusivamente del ámbito militar, de defensa e inteligencia, sino también que se enmarque en el reconocimiento y respeto por los derechos fundamentales de los ciudadanos y los estándares internacionales de derechos humanos como presupuesto de la ciberseguridad, evitando copiar literalmente las prácticas de otras regiones y de países que se encuentran en contextos diferentes a los nuestros.

En base al trabajo expuesto en el presente informe, consideramos elemental remarcar desde la sociedad civil algunas recomendaciones en torno al desarrollo de políticas públicas de ciberseguridad.

Teniendo en cuenta que América Latina aún puede avanzar hacia una perspectiva de la ciberseguridad respetuosa por los derechos humanos, los Estados deben propiciar el diálogo y el debate en foros que les permitan compartir sus experiencias y herramientas, con el fin de consolidar estándares que fortalezcan no solo

la ciberseguridad de cada país, sino regionalmente.

Los campos de acción de los organismos de inteligencia y ciberdefensa deben estar claramente delimitados, con miras hacia la transparencia y la rendición de cuentas por sus órganos de control, para evitar que a través del secreto se oculten prácticas ilegales así como la ineficacia del trabajo llevado a cabo por los mismos.

Teniendo en consideración la llegada de nuevas autoridades a cargo de los distintos aspectos de la ciberseguridad dentro del Ministerio de Modernización, así como también a la Dirección Nacional de Protección de Datos Personales (DNPDP), es fundamental replantear la dinámica de funcionamiento en torno a las políticas de ciberseguridad en conjunto con el proceso de reflexión para una reforma de la Ley de Protección de Datos Personales (LPDP) que busca impulsar las autoridades de la Dirección.

Así mismo, debe aprovecharse esta oportunidad para actualizar, mejorar y profundizar los programas de capacitación introducidos en años posteriores, como Internet Sano y Con Vos en la Web, los cuales juegan un rol sumamente importante al brindar y mejorar el nivel fundamental de seguridad digital de los ciudadanos.

En el pasado, los organismos del Estado encargados de impulsar las políticas de ciberseguridad mantuvieron una postura cerrada y poco transparente en su funcionamiento y su trabajo, manteniéndose alejados no solo de la ciudadanía, sino también de las comunidades expertas. Para asegurar un pleno desarrollo de políticas públicas de ciberseguridad, que alcance a todos los estratos de la sociedad, y que cuente con una mirada necesariamente holística, es fundamental involucrar al resto de los actores de la sociedad para que colaboren en el planteamiento e implementación de las mismas, tanto al sector privado, como a la comunidad técnica, academia y sociedad civil.

Estos ejes deben estar encaminados a conseguir un ecosistema sustentable de ciberseguridad, que permita a los ciudadanos desarrollar una vida segura online, al momento de hacer trámites, de realizar compras o en su día a día en la web; que los organismos públicos y privados respeten los datos personales y mantengan el adecuado resguardo y control de las bases de datos en respeto a la LPDP;

que los distintos estratos del Estado mantengan el mismo nivel de protección de sus infraestructuras y de resguardo de la información que manejan y almacenan; que organismos como la Unidad Fiscal Especializada en Cibercrimen (UFECI) cuenten con los recursos necesarios para afrontar los desafíos que suponen estos tipos delictuales y brindar estadísticas confiables que ayuden a pulir las políticas de ciberseguridad; que el equipo de respuesta a incidentes cibernéticos pueda trabajar eficazmente, recibiendo reportes y denuncias de todos los actores de la sociedad, pudiendo asesorar y ayudar a quienes se vean en la necesidad.


por los Derechos Civiles