INTEGRANDO ESTRATEGIAS DE CIBERDEFENSA MEDIANTE UNA PROPUESTA DE TRABAJO

WALTER FABIÁN AGÜERO*

MERCEDES CAROLINA VALLEJO*

Introducción

Muchas instituciones públicas y privadas adquieren modernos y sofisticados equipamientos de seguridad informática que, a pesar de esta previsión, suelen verse sobrepasadas por distintos ataques cibernéticos. La denegación de servicios distribuidos (DDoS), es uno de los flagelos que más repercusión y efectividad tienen sobre infraestructuras críticas[1]. En muchos casos, los ataques –que se propician con herramientas que se consiguen a precios económicos– provocan daños considerables al ecosistema del ciberespacio.

Estos actos vandálicos provocan enormes pérdidas económicas y operativas que ponen en peligro la normal funcionalidad de un país.[2]

* Magister en Ingeniería del Software. Doctorando en Ingeniería Informática (Universidad Nacional de San Luis).

* Técnica Superior en Periodismo.

1. https://elpais.com/tecnologia/2018/03/05/actualidad/1520249257_684529.html (publicación 5/3/2018)

2. Explosión en el sistema de distribución de gas en la URSS (1982), el ciberataque contra empresas estadounidenses conocido como Titan Rain (2003 – 2005), el ciberataque contra Estonia (2007), el ciberataque contra Siria (2007), las acciones de ciberguerra durante la guerra en Osetia del Sur (2008) y el ciberataque contra el programa nuclear iraní (2010) han constituido episodios destacados de ciberguerra (Torres, 2013)

Hace unas semanas, Europol[3], junto a otras fuerzas de ciberseguridad de distintos países, logró desmantelar el sitio web webstresser.org, la web más importante de ataques de denegación de servicio distribuidos (DDoS) que alcanzó los seis millones de ciberataques perpetrados por usuarios provenientes de Holanda, Italia, España, Croacia, Reino Unido, Australia, Canadá y Hong Kong. Este servicio ilegal fue cerrado e incautaron su infraestructura en Holanda, EE.UU. y Alemania.

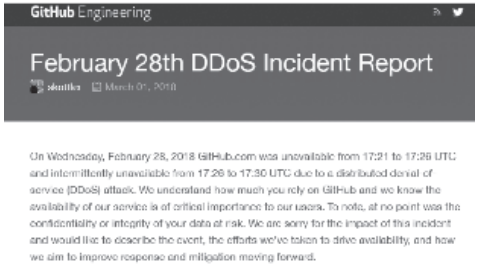
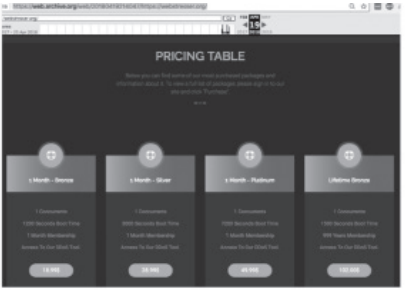


Imagen del sitio de GitHub[4]

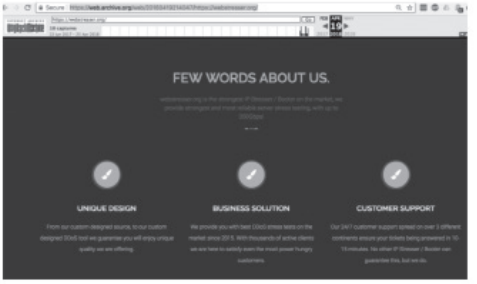
3. https://www.europol.europa.eu/newsroom/news/world%E2%80%99s-biggest-marketplace-selling-internet-paralysing-ddos-attacks-taken-down

4. https://githubengineering.com/ddos-incident-report/

En la tabla de la siguiente imagen, puede observarse el precio económico para realizar ataques de denegación de servicios distribuidos desde el sitio web Webstresser. Estos valores corresponden al 19 de abril de 2018, justo antes de que fuera cerrado. Los miembros de categoría “bronce” pagaban 15€ o 18.99$ al mes, que subían hasta 49,99$ mensuales por los servicios “platinum”.



Los servicios que ofrecían eran muy profesionales y algunos incluían:



Webstresser llegó a tener al mes de cierre del sitio más de 136.000 usuarios registrados, era el servicio DDos más profesional que había visto la Unidad contra Cibercrimen de Holanda[5]. Publicitaban ataques de hasta 350 Gbps, que es una potencia considerable. A modo de comparación, el mes pasado vimos el mayor ataque DDoS

5. https://news.sophos.com/es-es/2018/05/03/desmantelada-la-mayor-web-de-ataques-ddos/

de la historia, que alcanzó un máximo de 1350 Gbps, con una continuación de 400 Gbps.

Como se mencionó anteriormente, distintas entidades públicas y privadas ven con preocupación los riesgos que corren sus infraestructuras críticas y toman medidas de protección adquiriendo novedosos e innovadores recursos tecnológicos que les aseguren la protección de sus activos y les permitan, al menos por un cierto período de tiempo, sentirse protegidos.

¿Se podría recomendar un equipamiento que brinde mejor protección?

Adquirir la última tecnología, tener recursos humanos altamente capacitados y entrenados en ciberseguridad alcanzaría para asegurar que los equipos comprados no tienen vulnerabilidades, puertas traseras e incluso, sin haber tenido la posibilidad de comprobar el firmware del dispositivo adquirido, podría afirmarse que el equipamiento es seguro y confiable. Si la respuesta, como he de esperar es no, entonces el problema aumentó, ya que no solo se tendrá que justificar el gasto ante la autoridad competente, sino que también será la hora de actualizar el curriculum vitae y, además, reconocerle mérito al hábil vendedor. Las siguientes dos imágenes son contundentes para entender lo comentado en este punto. Al pie de la primera, en el diario La Nación, dice: “El arsenal de recursos de la NSA va desde cables USB especialmente modificados hasta la intromisión en el BIOS de los equipos de comunicaciones de Cisco, Huawei y Juniper Fuente: Reuters”.

Este trabajo intentará plantear soluciones que aporten al paradigma de la seguridad informática, de modo que ayuden a mejorar el control del ciberespacio.


LA NACION

Los trucos de EE.UU. para implementar su espionaje electrónico masivo

Imagen obtenida del diario La Nación. (3/01/2014)


Cisco confirma la vulnerabilidad de la NSA: era y es posible acceder a la información

Imagen obtenida de publicación en Internet[7]

Estado del arte de la ciberdefensa/ciberseguridad en América Latina

En la actualidad, existen varios estudios sobre las estrategias nacionales de ciberseguridad y ciberdefensa en Hispanoamérica, como así también del resto del mundo. A fines de febrero de 2018 el Grupo de Estudios en Seguridad Internacional de la Universidad de Granada, España presentó una investigación sobre Estrategias de ciberseguridad de Colombia, Panamá, Paraguay, Costa Rica, Chi-

7.https://www.xataka.com/seguridad/cisco-confirma-la-vulnerabilidad-de-la-nsa-era-y-es-posible-acceder-a-la-informacion

le y México[8]. Dicho trabajo concluyó que la mayor parte de los Estados dispone de capacidad de respuesta ante ciberataques, pero lo cierto es que, sin contar los países caribeños, sólo estos seis países han diseñado una estrategia de ciberseguridad, según informe de la OEA (2017).

En América, la preocupación por la ciberseguridad va tornándose prioritaria y, como muestra la siguiente imagen, la República Dominicana acaba de iniciar su Programa de ciberseguridad[9]. La toma de conciencia e importancia en el tema va cubriendo todo el continente.

El informe de la Universidad de Granada manifiesta que a excepción de los seis países que han aprobado este tipo de Estrategia hay dos factores que bloquean su adopción para que sea una realidad en el resto de América. Son:

1) la falta de recursos dedicados a este tema; y

2) la carencia de experiencia práctica y conocimientos especializados para diseñar e implementar este tipo de medidas".

Argentina es una rara excepción, ya que actualmente cuenta con doce recursos humanos que no están siendo utilizados y que fueron formados con el grado académico de Especialistas en ciberseguridad[10] en Corea del Sur.

7.https://www.xataka.com/seguridad/cisco-confirma-la-vulnerabilidad-de-la-nsa-era-y-es-posible-acceder-a-la-informacion

8.http://www.seguridadinternacional.es/?q=es/content/estrategias-nacionales-de-ciberseguridad-en-am%C3%A9rica-latina

9. https://twitter.com/OEA_RDominicana/status/993480503432044545

10. Korea University (CyberSecurity Specialist).

Proteger y cuidar el ciberespacio es un deber en conjunto de los sectores públicos y privados por lo que es necesario armar una estrategia de Seguridad Nacional que los coordine mediante claras políticas en común.

Estrategias de ciberseguridad de algunos países de América Latina

Colombia: Política Nacional de Seguridad Digital

Fue el primer país latinoamericano en aprobar una Estrategia Nacional de ciberseguridad en 2011 que, desde 2016, se llama Política Nacional de Seguridad Digital. El objetivo general de la Estrategia es fortalecer las capacidades de las múltiples partes interesadas para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital, en un marco de cooperación, colaboración y asistencia. Lo anterior es con el fin de contribuir al crecimiento de la economía digital nacional, lo que a su vez impulsará una mayor prosperidad económica y social en el país. (CONPES, 2016: 47).

Recientemente, del 7 al 11 de mayo, este país, junto a la OEA, países bajos y Canadá organizaron el curso "Proceso de La Haya: Operaciones de Seguridad Internacional y Ciberespacio", con la participación de 40 representantes del sector público y privado de América Latina.[11]

11. http://gobiernodigital.gov.co/623/w3-article-73372.html

Panamá: Estrategia Nacional de Seguridad Cibernética y Protección de Infraestructuras Críticas

El objetivo del Estado panameño es aunar los esfuerzos de sus ciudadanos, empresas e instituciones públicas para incrementar la seguridad cibernética y permitir el uso confiable de las tecnologías de la información en todos los ámbitos nacionales, salvaguardando los derechos y libertades fundamentales de los ciudadanos y un entorno económico regulatorio favorable al crecimiento y desarrollo de las empresas y permitiendo el buen funcionamiento del Estado. (Consejo Nacional para la Innovación Gubernamental, 2013: 3).

Paraguay: Plan Nacional de Ciberseguridad

La Política Nacional presenta una diferencia con el resto respecto de los objetivos. En las otras Estrategias Nacionales de ciberseguridad aparece un objetivo general y varios objetivos específicos (con excepción de la de Panamá). En cambio, en el caso de Paraguay aparecen una serie de objetivos generales bajo el nombre de ejes, dentro de los cuales se detallan 20 objetivos específicos para su consecución y 60 líneas de acción. Concretamente, son siete los ejes que se plantean:

- Sensibilización y cultura
- Investigación, desarrollo e innovación.
- Protección de infraestructuras críticas.
- Capacidad de respuesta ante incidentes cibernéticos.
- Capacidad de Investigación y Persecución de la Ciberdelincuencia.
- Administración Pública.
- Sistema Nacional de Ciberseguridad.

Costa Rica: Estrategia Nacional de Ciberseguridad

Se establece un objetivo general y ocho específicos, cada uno de los cuales comprende una serie de líneas estratégicas, sumando éstas un total de 20. En cuanto al objetivo general, se pretende desarrollar un marco de orientación para las acciones del país en materia de seguridad en el uso de las TIC, fomentando la coordinación y cooperación de las múltiples partes interesadas y promoviendo medidas de educación, prevención y mitigación frente a los riesgos en cuanto al uso de las TIC para lograr un entorno más seguro y confiable para todos los habitantes del país. (MICITT, 2017: 38).

Chile: Política Nacional de Ciberseguridad

Su política tiene como horizonte seis objetivos para el año 2022. Además, incluye un apartado con 41 medidas de política pública a llevar a cabo en el periodo 2017–2018.

1. Desarrollar una infraestructura de las TIC que, bajo una óptica de gestión de riesgos, sea capaz de resistir y recuperarse de incidentes de ciberseguridad.
2. Garantizar los derechos de los ciudadanos en el ciberespacio.
3. Desarrollar una cultura de ciberseguridad en torno a la responsabilidad en el uso de las TIC, a las buenas prácticas y a la educación.
4. Establecer relaciones de cooperación con otros actores en materia de ciberseguridad y participar de forma activa en foros internacionales.
5. Desarrollar una industria de la ciberseguridad chilena, que sea útil a los objetivos estratégicos del país.

México: Estrategia Nacional de Ciberseguridad

El Gobierno mexicano reconoce que el coste de los delitos informáticos a nivel global está ascendiendo y señala que, para el caso

de México, dicho coste fue de 3.000 millones de dólares en el año 2014. Además, indica que en los últimos años se ha producido un aumento exponencial de fraude cibernético. Es en este contexto donde surge la necesidad de adoptar dicha Estrategia.

México plasma tres principios rectores, establece un objetivo general y cinco estratégicos, define ocho ejes trasversales e identifica a los actores involucrados.

Los principios rectores son los siguientes: 1) Perspectiva de derechos humanos, que debe estar presente en cada una de las acciones en materia de ciberseguridad que se lleven a cabo en el marco de la Estrategia; 2) Enfoque basado en gestión de riesgos, es decir, un enfoque de prevención basado en la capacitación de los usuarios a fin de minimizar los riesgos y las amenazas del ciberespacio; y 3) Colaboración multidisciplinaria y de múltiples actores, para conseguir que la Estrategia se desarrolle de forma integral y transversal.

Argentina

Si bien el informe de la Universidad de Granada no menciona a Argentina, a continuación se describirá lo que desde el gobierno nacional se ha implementado:

Normativa legal

El Gobierno creó un Comité de ciberseguridad[12] con el objetivo de desarrollar una estrategia nacional que proteja el ciberespacio y tenga la capacidad de responder a incidentes de gran escala, a la vez que legisle en la materia. Lo hizo a través del Decreto 577/2017 publicado en el Boletín Oficial[13] (31/07/2017) con las firmas del presidente Mauricio Macri; el jefe de Gabinete Marcos Peña y los ministros Patricia Bullrich, Andrés Ibarra y Oscar Aguad.

12. https://www.boletinoficial.gob.ar/#!DetalleNorma/168225/20170731

13.http://servicios.infoleg.gob.ar/infolegInternet/verNorma.do;jsessionid=73DD1D96C41BF9215DF6F2E466E9B483?id=277518

El Comité de ciberseguridad se creó en la órbita del Ministerio de Modernización, que estará integrado por representantes del citado Ministerio (presidido por el Ministro), del Ministerio de Defensa y del Ministerio de Seguridad, el cual tendrá por objetivo la elaboración de la Estrategia Nacional de ciberseguridad. En la siguiente imagen se muestran gráficamente los Ministerios involucrados[14].

Son tareas del Comité de Ciberseguridad

• Desarrollar la Estrategia Nacional de Ciberseguridad, en coordinación con las áreas competentes de la Administración Pública Nacional.

• Elaborar el plan de acción necesario para la implementación de la Estrategia Nacional de Ciberseguridad.

• Convocar a otros organismos para que participen en la implementación de medidas en el marco del plan de acción elaborado conforme lo establecido en el punto precedente.

• Impulsar el dictado de un marco normativo en materia de ciberseguridad.

• Fijar los lineamientos y criterios para la definición, identificación y protección de las infraestructuras críticas nacionales.

• Participar en el desarrollo de acciones inherentes a la ciberseguridad nacional que se le encomienden.

14. https://www.argentina.gob.ar/sites/default/files/cofemod_comisionciberseguridad_el_panorama_de_la_ciberseguridad_en_numeros_12-08-16.pdf

Los ejes de trabajo que se plantearon inicialmente se pueden ver en la siguiente imagen, que pertenece a la misma referencia.

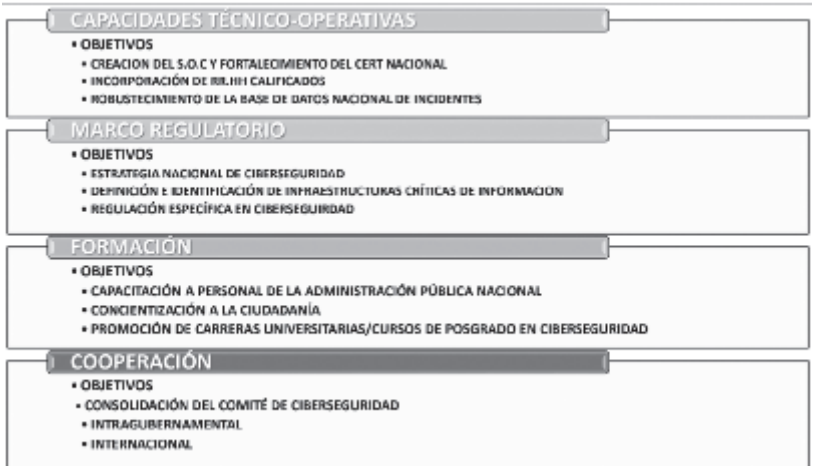


Imagen del panorama de la ciberseguridad de Argentina.gob

Programa Nacional de Infraestructuras Críticas de Información y ciberseguridad.

También crea el "Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad[15]" (ICIC), creado mediante la Resolución JGM Nº 580/2011 (28/7/2011). Éste tiene como finalidad impulsar 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.

15. http://www.icic.gob.ar/ y
http://servicios.infoleg.gob.ar/infolegInternet/anexos/185000-189999/185055/norma.htm

Normativas del Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad.

• Ley N° 26.388[16]: Ley que modifica el Código Penal a fin de incorporarle diversos delitos informáticos, tales como la distribución y tenencia con fines de distribución de pornografía infantil, violación de correo electrónico, acceso ilegítimo a sistemas informáticos, daño informático y distribución de virus, daño informático agravado e interrupción de comunicaciones.

• Resolución JGM Nº 580/2011[17]: crea el Programa Nacional de Infraestructuras Críticas de Información y ciberseguridad.

• Disposición ONTI Nº 3/2011[18]: aprueba el "Formulario de adhesión al Programa Nacional de Infraestructuras Críticas de Información y ciberseguridad", mediante el cual las entidades y jurisdicciones definidas en el artículo 8º de la Ley Nº 24.156 y sus modificatorias, los organismos interjurisdiccionales, y las organizaciones civiles y del sector privado podrán adherir al ICIC.

• Disposición ONTI 2/2013[19]: crea el grupo de trabajo "ICIC - CERT" (Computer Emergency Response Team) en el marco del "Programa Nacional de Infraestructuras Criticas de Información y ciberseguridad", y bajo la órbita de la Oficina nacional de Tecnologías de Información.

• Disposición ONTI 03/2013[20]: aprueba la "Política de Seguridad de la Información Modelo".

• Ley N° 26.904[21]: ley que incorpora al Código Penal la figura del ciberhostigamiento.

• Resolución PGN N° 2035/2014[22]: designa al Sr. Fiscal de la Procuración General de la Nación, Dr. Horacio Juan Azzolin, como "punto focal" de la Procuración General de la Nación en materia de Ciberdelincuencia.

16. http://www.infoleg.gob.ar/infolegInternet/anexos/140000-144999/141790/norma.htm
17. http://www.infoleg.gov.ar/infolegInternet/anexos/185000-189999/185055/norma.htm
18. http://www.infoleg.gov.ar/infolegInternet/anexos/185000-189999/187698/norma.htm
19. http://www.infoleg.gob.ar/infolegInternet/anexos/215000-219999/219212/norma.htm
20. http://www.infoleg.gob.ar/infolegInternet/anexos/215000-219999/219163/norma.htm
21. http://www.infoleg.gob.ar/infolegInternet/anexos/220000-224999/223586/norma.htm
22. http://www.icic.gob.ar/docs/PGN-2035-2014-001.pdf?id=244566

• Ley N° 27. 126[23]: crea la Agencia Federal de Inteligencia.

• Decisión Administrativa JGM N° 15/2015[24]: modifica la estructura organizativa del Ministerio de Defensa, incorporando la Dirección General de Ciberdefensa, cuya responsabilidad primaria y acciones se detallan en el cuerpo de la norma.

• Decreto N° 1067/2015[25]: crea la Subsecretaria de Protección de Infraestructuras Criticas de Información y Ciberseguridad y la Dirección Nacional de Infraestructuras Criticas de Información y Ciberseguridad, ambas dependientes de la Secretaria de Gabinete de la Jefatura de Gabinete de Ministros.

• Decreto N° 1311[26]: aprueba la "Nueva Doctrina de Inteligencia Nacional".

• Resolución JGM N° 1046/2015[27]: aprueba la estructura organizativa de la Dirección Nacional de Infraestructuras Criticas de Información y Ciberseguridad, dependiente de la Subsecretaria de Protección de Infraestructuras Criticas de Información y Ciberseguridad de la Secretaria de Gabinete de la Jefatura de Gabinete de Ministros.

Aportes académicos

En distintos países de América, se están llevando capacitaciones de posgrado en ciberseguridad y/o ciberdefensa. Como ejemplo, Colombia y Argentina ofrecen maestrías. Se destaca también la Ingeniería en ciberseguridad que comenzó a dictarse este año en varias regiones de Chile y el doctorado en temas relacionados a la ciberseguridad y la ciberdefensa en la Universidad Nacional de San Luis.

En distintos congresos nacionales e internacionales, se observan con mayor frecuencia la presentación de trabajos relacionados a algún tema en ciberseguridad de investigadores argentinos. Estos son solo

23. http://www.infoleg.gob.ar/infolegInternet/anexos/240000-244999/243821/norma.htm

24.http://www.infoleg.gob.ar/infolegInternet/verNorma.do;jsessionid=612F1B2A90F0F9D4627BCA6D21C-DD81B?id=244566

25. http://www.infoleg.gob.ar/infolegInternet/anexos/245000-249999/247971/norma.htm

26.http://www.infoleg.gob.ar/infolegInternet/verNorma.do;jsessionid=612F1B2A90F0F9D4627BCA6D21C-DD81B?id=248914

27. http://www.infoleg.gob.ar/infolegInternet/anexos/250000-254999/251022/norma.htm

algunos ejemplos que muestran la preocupación de los países en el tema de protección cibernética.

Aportes no académicos

En algunas provincias argentinas, funcionan empresas de seguridad internacionales no argentinas con base en otros países. Sus empleados, así como investigadores independientes de distintos ámbitos, difunden materiales relacionados a seguridad informática en encuentros no académicos, es decir, en los que no representan a ninguna universidad.

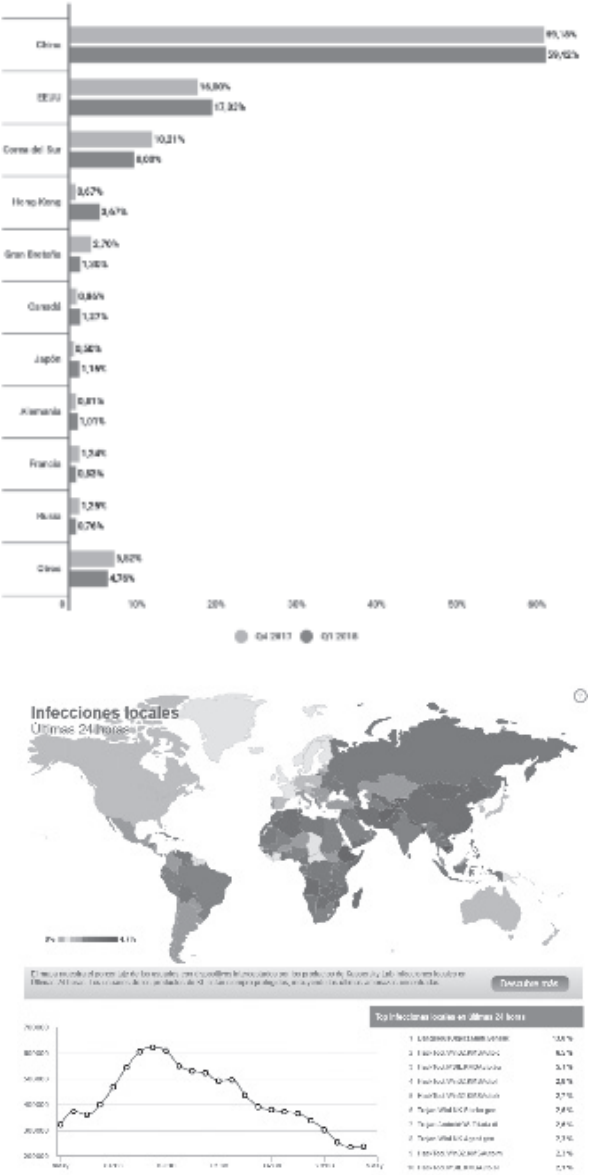
Cómo conclusión del estado del arte, se puede decir que una Estrategia de ciberseguridad no garantizará que se puedan repeler o prevenir los ataques, pero su ausencia trae consecuencias negativas al ciberespacio.

Amenazas y ataques

Diversos reportes mundiales informan de los distintos peligros a los que nos enfrentamos en el ciberespacio, advirtiendo con proyecciones anuales de los peligros a los que nos podríamos enfrentar[28]. También existen herramientas que permiten ver en tiempo real los distintos tipos de ataques e identificar a quienes los llevan a cabo.

En la siguiente imagen se muestra, a modo de ejemplo, un informe del primer trimestre (Q1) de la empresa Kaspersky:

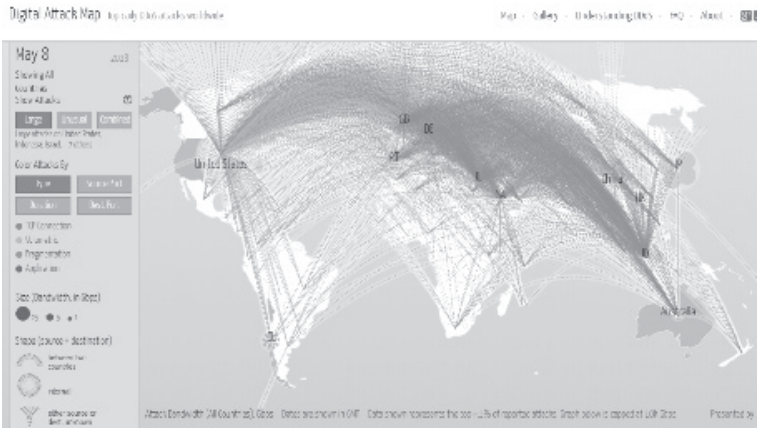
28.https://latam.kaspersky.com/blog/kaspersky-lab-presenta-su-pronostico-de-ciberseguridad-del-2018-para-america-latina/12142/



Geografía de los ataques de DDoS[29]

29. https://securelist.lat/ddos-report-in-q1-2018/86887/

Otros muestran las infecciones según tipo de virus (la imagen corresponde al 10/05/2017).



Algunos de los sitios que nos muestran en tiempo real los ataques de DDoS son:

a) http://www.digitalattackmap.com/

b) https://cybermap.kaspersky.com/

c) http://www.norse-corp.com/

Otros reportes evalúan la protección en tiempo real que realizan los más importantes antivirus[30] y que son elaborados por AV Comparatives, quien realiza distintos tipos de test sobre los antivirus. A título de ejemplo, mencionaremos: prueba de protección en el mundo real, prueba de rendimiento, prueba de protección contra malware, prueba de alarma falsa y prueba de eliminación de malware[31], etc.

La siguiente imagen muestra una clasificación según el siguiente nivel:

• STANDARD requiere que un programa alcance un buen estándar, aunque indica áreas que necesita una mejora adicional en comparación con otros productos.

30. http://www.av-comparatives.org/dynamic-tests/

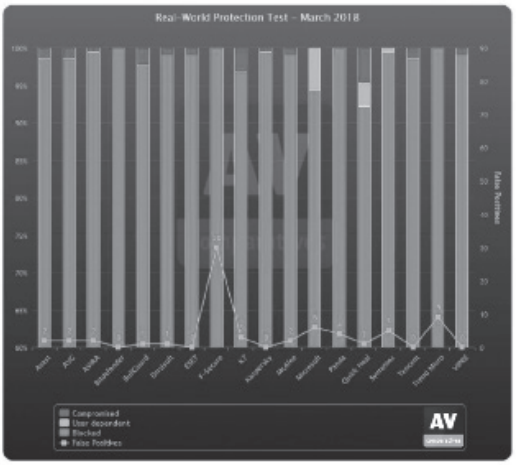
31. http://www.av-comparatives.org/comparatives-reviews/

• AVANZADO indica áreas que pueden necesitar alguna mejora, pero ya son muy competentes. A continuación, se muestra un resumen de los premios alcanzados por varios productos antivirus en la serie principal de pruebas de consumo de AV-Comparatives de 2017.

	Malware Protection	Performance	Real-World Protection	Malware Removal	Malware Protection	Performance	Real-World Protection
	March 2017	May 2017	February-June 2017	February-October 2017	September 2017	October 2017	July-November 2017
Bitdefender	***	***	***	***	***	***	***
Kaspersky Lab	***	***	***	***	***	***	***
VIPRE	***	**	***	***	***	***	***
Avira	***	***	***	**	**	***	***
Avast	**	***	***	**	***	***	***
AVG	**	***	***	**	***	***	***
Tencent	***	***	***	***	**	**	***
eScan	***	***	**	***	***	***	*
ESET	*	***	**	**	***	***	***
F-Secure	***	**	**	**	**	***	**
Emsisoft	**	***	*	**	***	**	***
BullGuard	***	*	**	**	***	***	**
Panda	***	**	***		**	***	***
McAfee	*	***	*		***	***	***
Trend Micro	**	*	**	**	*	**	***
Seqrite	**	***	tested	*	***	***	*
Symantec	tested	***	***		tested	***	**
Adaware	**	*	**	**	***	*	tested
Fortinet	tested	**	**	*	*	**	**
CrowdStrike	tested	**	**		tested	**	**
Microsoft	*	*	**	*	tested	*	**

Key: * = Standard, ** = Advanced, *** = Advanced+

Siguiendo la misma línea de análisis, tenemos el siguiente cuadro que aclara el anterior



http://www.av-comparatives.org/wp-content/uploads/2018/04/avc_factsheet2018_03.pdf

	OFFLINE Detection Rate	ONLINE Detection Rate	ONLINE Protection Rate	False Alarms
Avast	89.4%	99.5%	100%	9
AVG	89.4%	99.5%	100%	9
AVIRA	97.4%	99.5%	99.99%	1
Bitdefender	98.8%		99.99%	2
BullGuard	98.8%		99.93%	5
Emsisoft	98.8%		99.98%	7
ESET	97.9%		99.82%	1
F-Secure	98.8%	99.3%	99.93%	10
K7	97.7%	98.2%	99.81%	88
Kaspersky Lab	94.5%	97.8%	99.98%	9
McAfee	77.9%	99.2%	99.95%	10
Microsoft	92.8%	99.9%	99.99%	70
Panda	40.5%	82.1%	99.99%	327
Quick Heal	98.8%		99.81%	8
Symantec	91.4%	99.9%	99.99%	90
Tencent	98.8%		100%	93
Trend Micro	43.3%	99.7%	100%	166
VIPRE	98.8%		99.96%	5
average	*89.1%*	*98.1%*	*99.95%*	*50*
min	*40.5%*	*82.1%*	*99.81%*	*1*
max	*98.8%*	*99.9%*	*100%*	*327*

Cómo se puede observar, existen diversas herramientas que nos permiten observar en tiempo real cómo se están llevando a cabo distintos tipos de ciberataques entre naciones y otros organismos que evalúan programas antivirus.

Retomando la cuestión sobre la posibilidad de recomendar el equipamiento que brinde la mejor protección, en relación de lo comentado en el párrafo anterior, me surgen distintas preguntas: ¿cómo se llevan a cabo estas acciones?; ¿de dónde se toman las fuentes de datos?; si en algún momento, mirando las herramientas de tiempo real, vemos que somos atacados desde un determinado país, ¿nos puede servir como recurso forense?

Una alarma "alarmante"

Brevemente, y siguiendo la lógica del documento, se podrá afir-

mar que todo el esfuerzo realizado en materia legal, estructural, etc. sobre acciones de ciberseguridad y ciberdefensa en algún momento llegará a depender de equipamientos tecnológicos sobre los que no hay certeza de si "son seguros" y, como si fuera poco, tampoco del software que se usará. A esta altura, lo único cierto es que fue muy afortunado el vendedor de la tienda que encontró buenos compradores. ¿Será realidad esto que se menciona?

A continuación, una imagen del blog Apple[32] de Eleven Paths[33], publicada hace unos días (8/5/2018), muestra que la compañía Apple sigue resistiendo a las propuestas del FBI y su *backdoor*.

A esta altura, todo parece un panorama nada alentador para la ciberseguridad, pero no todo es para preocuparse. en el próximo punto se plantean soluciones para ser discutidas.

Antecedentes exitosos

Otros países de habla hispana, como España, tienen un rotundo éxito en empresas de ciberseguridad, como es el caso de la citada Eleven Paths. Según un informe que publica Business Insider de España[34] es sólo una de las diez mejores empresas de ciberseguridad

32. http://www.seguridadapple.com/2018/05/apple-sigue-resistiendo-las-propuestas.html

33. Eleven Paths https://www.elevenpaths.com , División de Ciberseguridad de Telefónica de España.

34.https://www.businessinsider.es/principales-empresas-espanolas-dedicadas-ciberseguridad-201230

de ese país, que nació en el año 2013 gracias a un proyecto de su fundador, Chema Alonso (ver foto en la imagen siguiente) con ideas semejantes a las que aquí se verterán.

Otra empresa del mismo rubro de ciberseguridad, y que forma parte del mismo informe, es el antivirus Panda, nacido en 1990 en Bilbao.

Planteando soluciones

Comparada con otros países de América Latina, Argentina tiene la fortaleza de contar con un gran número de especialistas en distintas áreas de la ciberseguridad. Además, cuenta con algunas infraestructuras que dependen del Estado nacional, así como de estados provinciales aptas para ser bases de trabajo en ciberdefensa/ciber-

seguridad, lo que hacen pensar que unir este potencial convertiría en un desafío inspirador del desarrollo tecnológico del país en este tema.

Los recursos humanos existentes en Argentina se distribuyen aproximadamente en:

1. Empresas internacionales en ciberseguridad radicadas en Argentina cuentan con recursos humanos argentinos que produce desarrollos de software, en algunos casos para éstas, en distintas áreas específicas del tema.

2. Investigadores de distintas universidades del país trabajan en sus tesis sobre ciberseguridad/ciberdefensa para alcanzar el grado académico de maestría y/o doctorado.

3. Existen algunos investigadores informales que conocen y trabajan a tiempo parcial en ciberseguridad.

4. En Corea del Sur, se formó un equipo de 12 personas como *cybersecurity specialists* (Korea University). Actualmente, la capacidad de esos recursos humanos no está siendo aprovechada.

El siguiente cuadro resume cómo los recursos humanos trabajan desarticuladamente en ciberdefensa y ciberseguridad nacional.

La seguridad informática es un requisito primordial del ámbito privado y público. Por ello, es necesario fijar objetivos claros y urgentes. A continuación, algunos de ellos:

1. Fijar pautas para el cumplimiento de seguridad de los sistemas de información, comunicación e infraestructura crítica de los dos sectores.

2. Fijar acciones de capacitación con prioridad en todas las dependencias críticas pertenecientes al sector público y privado (policía, universidades, Poder Judicial, empresas).

3. Fijar protocolos de detección, respuesta, forense digital y coordinación de actividades de ciberterrorismo, hacking, ciberespionaje, sabotajes, amenazas internas, etc.

4. Fijar protocolos de recuperación ante ataques de entidades mencionadas en el punto 2.

5. Fijar lineamientos de capacitación a la población.

6. Establecer los protocolos de colaboración internacional, así como entre provincias y empresas.

7. Fijar lineamientos para la compra y adquisición de equipamiento para infraestructura crítica (hardware y/o software) de seguridad que permitan tener cierto control sobre el firmware y/o BIOS, etc. de modo tal que se cumplan estándares de seguridad y especificaciones técnicas de los equipos que se adquieran en materia de ciberseguridad antes de que el fabricante los entregue para su evalución.

8. Desarrollo de aplicaciones nacionales cuyos códigos fuentes sean auditables.

9. Análisis del software y equipamiento de seguridad existente (recordar caso: Estados Unidos vs Karsperky)[35].

Además, debería existir un organismo independiente que coordine líneas de acción con las fuerzas de seguridad nacional y Presidencia que, cumpliendo funciones similares a las anteriormente citadas, las ordene e impulse líneas de desarrollo e investigación con distintas universidades a efectos de tener proyectos propios de ciberdefensa/ciberseguridad desarrollados por tesistas de maestrías y/o doctorados de dichas universidades.

Otro de los puntos fundamentales es tener capacidad de desarrollo que permitan:

1. Tener un sistema de alerta temprana de detección de amenazas e incidentes en el tráfico de cualquier red existente.

35. https://www.cnet.com/es/noticias/trump-decreto-prohibicion-kaspersky/
http://www.bbc.com/mundo/noticias-internacional-41262944

2. Contar con equipos de formación de recursos humanos para el combate de la ciberguerra (igual al *Best of the best* de Corea del Sur).

3. Tener un equipo que desarrolle un antivirus para toda clase de dispositivos.

4. Desarrollar herramientas de análisis de archivos con potencial código malicioso (sandboxing).

5. Desarrollo de equipos de competición nacional en ciberseguridad en busca de talentos en temas (criptografía, esteganografía, exploit, forense digital, análisis de tráfico, código reversing y hacking web).

6. Formación de cursos a distancia preparativos para la competencia comentada, como así también de concientización utilizando la técnica capacitador de capacitadores.

Es necesario tener una mirada parecida a la de una startup para nuestro país con líneas de acción concreta donde permita vincular experiencia, trabajos y áreas de desarrollo de una forma nueva de investigación y desarrollo en ciberseguridad que comprenda las distintas áreas de trabajo.

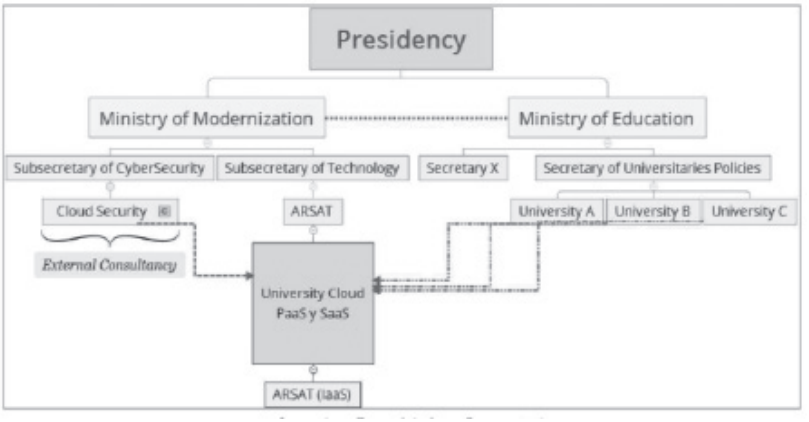
Conclusión

Como se mencionó anteriormente, Argentina cuenta con recursos humanos y tecnológicos para producir ciertas tecnologías vitales para el país. Esta producción lograría cubrir un espectro importante de nuestras necesidades en materia de ciberseguridad y ciberdefensa. Sólo hace falta, como en toda área, un director técnico con la visión que comparto en este trabajo que, sumada a la confianza y decisión política, permitan empezar a soñar en alcanzar a autoabastecernos de ciertas tecnologías de bandera nacional creadas por y para argentinos.

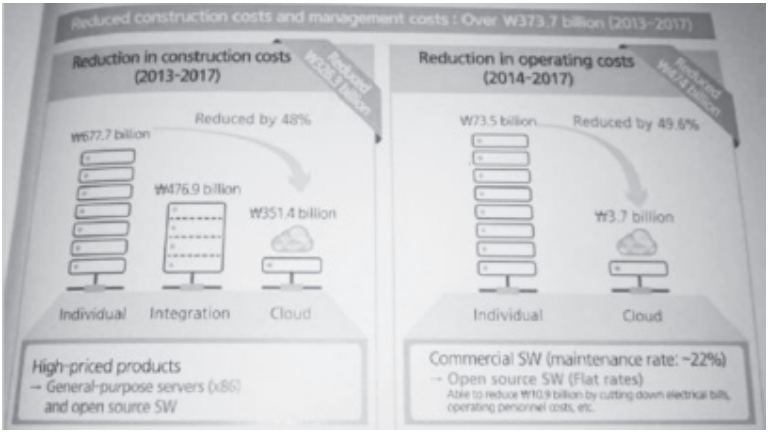
Para ejemplificar las destrezas que son propias de los argentinos, cito el ejemplo de una consultoría internacional aprobada por el gobierno de Corea del Sur, Korea University y Kait que permiten

aplicar ciberseguridad/ciberdefensa para lograr mejoras en la educación universitaria y el correspondiente ahorro de varios billones de dólares en un plazo de 10 años. Para realizarla, se utilizaron algunas dependencias de Estado nacional, como la de ARSAT. Existen, al menos, dos ejemplos más alcanzados por la misma certificación coreana que permiten afirmar que es posible darle una vuelta de rosca y transitar un acertado desarrollo tecnológico argentino en materia de ciberseguridad y ciberdefensa.

En la siguiente imagen, se ilustra parte del trabajo de consultoría internacional mencionado, del que fui co-autor.



La próxima imagen corresponde a la proyección de gasto evaluada dentro del contexto del mismo proyecto y que permite afirmar un ahorro importante. Dichos recursos pueden destinarse a otras áreas de la educación universitaria que los necesiten. El ahorro proyectado tiene como principal referencia la implementación de proyectos similares en otros países, como Corea de Sur.



Trabajos a realizar

Para lograr el cambio de paradigma, es necesario mirar alternativas, como por ejemplo las de mi trabajo de investigación: *Detección de Ciberataques de DDoS* utilizando Inteligencia Artificial en ambientes de Redes Definidas por Software (SDN: Sotware Defined Network).

Las redes SDN son actualmente utilizadas por empresas como Google[36], Amazon, Netflix y ésta les permite la administración por medio de desarrollos de programación propios usando, por ejemplo, lenguaje Python en sus equipos (Firewall, Machine Learning, Deep Learning, etc.).

Los ejemplos de casos de usos en empresas multinacionales mencionados hacen posible pensar en modelos alternativos y/o combinados a los tradicionales para la protección eficaz de nuestro ciberespacio.

36.https://www.blog.google/topics/google-cloud/making-google-cloud-faster-more-available-and-cost-effective-extending-sdn-public-internet-espresso/

Bibliografía

https://f5.com/products/security

http://www.cari.org.ar/pdf/ciberdefensa_riesgos_amenazas.pdf

https://www.uma.es/foroparalapazenelmediterraneo/wp-content/uploads/2014/07/dsegd_60.pdf

https://ccdcoe.org/training.html

https://latam.kaspersky.com/blog/kaspersky-lab-presenta-su-pronostico-de-ciberseguridad-del-2018-para-america-latina/12142/

Banco Interamericano de Desarrollo (BID) y Organización de los Estados Americanos (OEA) (2016). ciberseguridad ¿Estamos preparados en América Latina y el Caribe? Recuperado de: https://digital-iadb.leadpages.co/ciberseguridad-en-la-region/

Consejo Nacional para la Innovación Gubernamental (2013). Gaceta Oficial Digital. Nº 21. Estrategia Nacional de Seguridad Cibernética y Protección de Infraestructuras Críticas. Recuperado de: https://www.unodc.org/res/cld/lessons-learned/pan/estrategia_nacional_de_seguridad_cibernetica_y_proteccion_de_infraestructuras_criticas_html/Estrategia_Nacional_de_Seguridad_Cibernetica_y_Proteccion_de_Infraestructuras_Criticas.pdf

Documento CONPES 3854 (Consejo Nacional de Política Social y Económica) (2016). Política Nacional de Seguridad Digital. Recuperado de: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf

Gobierno de Chile (2017). Política Nacional de ciberseguridad. Recuperado de: http://ciberseguridad.interior.gob.cl/media/2017/05/PNCS-CHILE-FEA.pdf

Gobierno de México (2017). Estrategia de ciberseguridad. Recuperado de: https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_ciberseguridad.pdf

Leiva E. (2015). Estrategias Nacionales de ciberseguridad: Estudio comparativo basado en Enfoque Top-Down desde una visión global a una visión local. *Revista Latinoamericana de Ingeniería de Softwa-*

re, 3(4). pp. 161-176, ISSN 2314-2642. Recuperado de: http://sistemas.unla.edu.ar/sistemas/gisi/papers/relais-v3-n4-161-176.pdf

MICITT (2017). Estrategia Nacional de ciberseguridad de Costa Rica. Recuperado de: https://micit.go.cr/images/imagenes_noticias/10-11-2017__ciberseguridad/Estrategia-Nacional-de-ciberseguridad-de-Costa-Rica-11-10-17.pdf

Observatorio CISDE (2017). Pronóstico de ciberseguridad para América Latina en 2018. Recuperado de: https://observatorio.cisde.es/sin-categoria/pronostico-ciberseguridad-america-latina-2018/

OEA (2017). México presentó Estrategia Nacional de ciberseguridad desarrollada con apoyo de la OEA. Recuperado de: http://www.oas.org/es/centro_noticias/comunicado_prensa.asp?sCodigo=C-082/17

Secretaría Nacional de Tecnologías de la Información y la Comunicación (2017). Plan Nacional de ciberseguridad. Retos, roles y compromisos. Recuperado de: http://gestordocumental.senatics.gov.py/share/s/zkKW1CkKScSvapqlB7UhNg

Torres, M. (2013). Ciberguerra. En Jordán, J. (coord.), M*anual de Estudios Estratégicos y Seguridad Internacional.* pp. 329-348. Madrid: Plaza & Valdés.