Tema central

DOI: http://dx.doi.org/10.17141/urvio.20.2017.2859

URVIO, Revista Latinoamericana de Estudios de Seguridad, No. 20, Quito, junio 2017, pp. 8-15
RELASEDOR y FLACSO Sede Ecuador • ISSN 1390-4299 (en línea) y 1390-3691

Ciberseguridad. Presentación del dossier

Cybersecurity. Introduction to Dossier

Carolina Sancho Hirare[1]

Fecha de recepción: 24 de marzo de 2017
Fecha de aceptación: 15 de mayo de 2017

La gobernabilidad de todo sistema político requiere al menos considerar tres factores: seguridad como condición, institucionalidad como medio y desarrollo como objetivo. En este contexto, la ciberseguridad constituye una condición para permitir que los ciudadanos, las organizaciones e instituciones puedan beneficiarse del uso del ciberespacio como dimensión en la cual las relaciones sociales pueden efectuarse en forma más rápida y económica en comparación con otras formas conocidas de intercambio de información.

La ciberseguridad emerge ante el creciente uso del ciberespacio como nueva dimensión para la interacción social, resultado de la revolución de la tecnología de la información y comunicación (TIC), que ha acelerado el proceso de globalización y periódicamente sorprende con su constante innovación. Ejemplo de ello, lo encontramos en el incremento de la cantidad de aparatos conectados al ciberespacio, lo que ha dado origen a la denominada internet de las cosas. Asimismo, la gran cantidad de datos virtuales generados en el ciberespacio ha permitido el desarrollo de "big data" o grandes bases de datos que posibilitan almacenar ingentes cantidades de información y posibilitan el rápido análisis de grandes cantidades de datos de variable naturaleza o formato. El especialista a cargo de estas bases de datos es el "data scientist", un experto cada vez más demandado en el futuro, cuyo principal aporte es dar valor agregado a la información almacenada en "big data" a partir del análisis que puede efectuar en corto tiempo y con recursos limitados.

Estas nuevas tendencias se han potenciado por el aumento sostenido de personas conectadas al ciberespacio. Según cifras de la Unión Internacional de Telecomunicaciones (UIT), en 2015 a nivel mundial, la cantidad de usuarios de internet se ha estimado en un 40% de la población y los abonados a banda ancha móvil serían unos 3.500 millones de personas. Sin embargo, el creciente acceso a este recurso trae aparejado nuevos desafíos. Uno de ellos, es el efectivo uso de todo el potencial de internet, tal como indica la UIT (2016) en el reporte anual "Medición de la sociedad de la información":

1 Doctora en Conflictos, Seguridad y Solidaridad por la Universidad de Zaragoza. Profesora en la Academia Nacional de Estudios Políticos y Estratégicos (ANEPE) de Chile. Correo: csanchohirane@yahoo.es

Usuarios de internet con niveles educativos más altos utilizan servicios más avanzados, como los de cibercomercio y los servicios financieros y gubernamentales en línea, en mayor grado que los usuarios de Internet con niveles de educación e ingresos inferiores, quienes usan Internet sobre todo con fines lúdicos y comunicativos.

Por este motivo, no solo es necesario ofrecer acceso a internet, sino también se requiere que las autoridades encargadas de la elaboración de políticas aborden las desigualdades socioeconómicas generales y establezcan medidas que permitan a las personas adquirir las habilidades y competencias necesarias para el uso

Figura 1. Factores de riesgo en el Ciberespacio

Autoría	Objetivos	
	Gobierno	Sector Privado
Ataques patrocinados por otros Estados	Espionaje, ataques contra infraestructuras críticas, amenazas persistentes avanzadas (APT, por sus siglas en inglés)	Espionaje, ataques contra infraestructuras críticas, APT
Ataques patrocinados por privados	Espionaje	Espionaje
Terroristas, extremismo político e ideológico	Ataques contra redes y sistemas; contra servicios de Internet; infección con *malware*; contra redes, sistemas o servicios de terceros	Ataques contra redes y sistemas, ataques contra servicios de Internet, infección con malware, ataques contra redes, sistemas o servicios de terceros
Hacktivistas	Robo y publicación de información clasificada o sensible, ataques contra las redes y sistemas, ataques contra servicios de Internet, infección con malware, ataques contra redes, sistemas o servicios de terceros	Robo y publicación de información clasificada o sensible, ataques contra las redes y sistemas, ataques contra servicios de Internet, infección con malware, ataques contra redes, sistemas o servicios de terceros
Crimen organizado	Espionaje	Robo de identidad digital y fraude
Ataques de bajo perfil	Ataques contra las redes y sistemas, ataques contra servicios de Internet, infección con malware, ataques contra redes, sistemas o servicios de terceros	Ataques contra las redes y sistemas, ataques contra servicios de Internet, infección con malware, ataques contra redes, sistemas o servicios de terceros
Ataques de personal con accesos privilegiados (*Insiders*)	Espionaje, ataques contra infraestructuras críticas, ataques contra las redes y sistemas, ataques contra servicios de Internet, infección con malware, ataques contra redes, sistemas o servicios de terceros, robo y publicación de información clasificada o sensible, APT	Espionaje, ataques contra infraestructuras críticas, ataques contra las redes y sistemas, ataques contra servicios de Internet, infección con malware, ataques contra redes, sistemas o servicios de terceros, robo y publicación de información clasificada o sensible, APT
Impacto	**Alto**	
	Medio	
	Bajo	

Fuente: Instituto de Ciberseguridad de España (2012).

pleno de Internet. La creciente consideración del ciberespacio e internet como un bien público, obliga al Estado a desarrollar acciones necesarias que garanticen condiciones mínimas de seguridad –según estándares internacionales- para que toda la población pueda usarla en forma confiable.

En este sentido, es necesario reconocer que el aumento en el uso del ciberespacio, ha generado ventajas y desventajas para los usuarios. Sus cualidades de facilidad en el acceso, rapidez en la transmisión de la información y bajo costo en la comunicación se ha visto afectado por la existencia de riesgos que han puesto en cuestión la conveniencia de su uso en forma única por parte de personas organizaciones e instituciones, los cuales son sistematizados en la figura 1.

En efecto, periódicamente los ciudadanos reciben información sobre nuevos ciberdelitos ante los cuales muchas veces están desprotegidos, como es el caso del robo de información en formato electrónico; el "phishing" o acceso fraudulento de información personal a través del engaño, como por ejemplo, una clave de acceso a una cuenta desde una página falsa; el "ransomware" o secuestro de datos en el ciberespacio, que para recuperarlos se cobra un monto de dinero, muchas veces en la moneda virtual "bitcoin".

Figura 2. Las principales familias de malware de 2014

Familia de Malware	Descripción
KEYGEN	Genera números de serie para entrar a los programas que requieren números de serie válidos para que los programas funcionen completamente
DUNIHI	Esta Familia de malware normalmente es malware VBS ofuscado que es capaz de propagarse infectando unidades removibles; puede llegar como archivo anexo del correo no deseado.
ACTIVATOR	Quiebra la aplicación y el usuario puede instalarla mutualmente. Sus rutinas le permiten a los usuarios evadir las técnicas de registro y protección de las aplicaciones. Esto les permite utilizar la versión registrada de las aplicaciones.
DOWNAD/ Conficker	Esta explota una vulnerabilidad del servicio del servidor que, cuando es explotada, permite que un usuario remoto ejecute el código arbitrario en el sistema infectado para propagarse a las redes.
CONDUIT	Se incluye en los paquetes de malware como un componente de malware, como un archivo entregado por otro malware, o como un archivo que los usuarios descargan sin darse cuenta cuando visitan sitios maliciosos.
PRODUKEY	Una aplicación que muestra la identificación del producto y la clave del CD de cierto software si se instala en el sistema afectado. Esta herramiento de hackeo puede ser instalada manualmente por el usuario.
SAFNUT	Se incluye en los paquetes de malware como un componente de malware. Llega al sistema como un archivo entregado por otro malware o como un archivo que lo usuarios descargan sin darse cuenta cuando visitan sitios maliciosos.
AGENT	Normalmente trae consigo cargas o realiza otras acciones maliciosos, que van moderando desde moderadamente molestas hasta las irreparablemente destructivas. También pueden modificar las configuraciones del sistema para que se inicie automáticamente. Para restaurar los sistemas afectados podrían requerirse.
CROSSRDR	Se incluye en los paquetes de malware como un componente de malware. Llega al sistema como un archivo entregado por otro malware o como un archivo que los usuarios descargan sin darse cuenta cuando visitan sitios maliciosos.
FAKEAV	Crea carpetas en los sistemas afectados y entrega varios archivos, incluyendo una copia de sí mismo y un archivo malicioso. Realiza varios cambios al registro, uno de los cuales permite que se ejecute cada vez que el sistema arranca.

Fuente: Organización de Estados Americanos (OEA) y *Trend Micro* (2015).

Este ilícito, afectó a organizaciones en diversos lugares del mundo en forma simultánea, las cuales no habían actualizado sus equipos con los parches que las empresas de software habían colocado recientemente a disposición de sus clientes.

Se adiciona a lo señalado, las frecuentes noticias sobre ciberataques a diversas organizaciones afectando su normal funcionamiento, por ejemplo, cuando se produce un ataque de denegación distribuida de servicio (DDoS) o cuando un malware del tipo APT afectan los sistemas de supervisión, control y adquisición datos (SCADA) en la infraestructura crítica, como ocurrió con el gusano informático en el sistema de control de los reactores nucleares de Natanz en Irán. La figura 2, permite ilustrar la variedad de malware existentes. En ella son descritas las principales familias de malware detectadas en 2014, las que se han incrementado por mutación o por la aparición de nuevos software maliciosos.

Situaciones como las descritas, obligan a reconocer la importancia de la seguridad en el ciberespacio y asumir su complejidad, pues las amenazas en el ciberespacio pueden tener diversos orígenes (estatal o no estatal), pero el mismo efecto de perjudicar a las personas, dañar a las organizaciones e impedir el normal funcionamiento de instituciones. Asimismo, la existencia de ciberdelito, ciberataques, ciberespionaeje y posiblemente, la ciberguerra (ver figura 3) –no hay consenso entre los expertos en este concepto-, obliga a las máximas autoridades nacionales a contar

Figura 3. Episodios destacados de ciberguerra

Fecha	Denominación	Resumen
1982	Explosión en el sistema de distribución de gas (Unión Soviética)	Los servicios de inteligencia estadounidenses introdujeron una *bomba lógica* en un software de control de infraestructuras gasísticas que había sido robado por espías soviéticos a una empresa canadiense.
2003 2005	Titan Rain	Conjunto de ataques coordinados contra empresas estratégicas e instituciones estadounidenses presumiblemente procedentes de China.
2007	Ciberataque contra Estonia	La retirada en este país de una estatua del período soviético desencadena un conjunto de graves ataques procedentes de Rusia que afectan a las instituciones estatales, bancos y medios de comunicación.
2007	Ciberataque contra Siria	La aviación israelí bombardea una instalación nuclear secreta. El ataque aéreo fue precedido de un ciberataque que engañó a los sistemas de defensa aérea e impidió detectar la incursión de los aviones en el territorio sirio.
2008	Guerra en Osetia del Sur	De manera paralela al conflicto hubo ciberataques coordinados desde Rusia contra sitios gubernamentales de Georgia que quedaron inutilizados y tuvieron que ser reubicados en servidores de otros países.
2010	Stuxnet	Un troyano provoca la destrucción de maquinaria del programa nuclear iraní.

Fuente: Torres (2013).

con políticas públicas que regulen el empleo del ciberespacio y ofrezcan seguridad en su uso, como también el respeto de los derechos de los ciudadanos, los cuales se han visto en cuestionamiento frente a una tecnología capaz de obtener muchos datos sensibles de las personas, pero incapaz de resguardarlos adecuadamente.

Junto a lo indicado, resulta urgente la formulación de políticas públicas y/o estrategias nacionales de ciberseguridad que permitan sistematizar los principales objetivos nacionales e internacionales en la materia, explicitar las acciones que permitirán alcanzarlos y las metas que permitirán constatar su logro. En efecto, los gobiernos de los países son responsables de elaborar políticas que promuevan y garanticen adecuados niveles de ciberseguridad según estándares internacionales, especialmente en lo que dice relación con la protección de la infraestructura crítica de la información a nivel nacional.

Resulta recomendable que tanto las políticas como la estrategia de ciberseguridad sean desarrolladas en un ambiente de participación que contemple al sector público, privado, académico y la sociedad civil, pues condicionará su legitimidad, aspecto fundamental en el éxito de su posterior implementación. Especial mención requiere la participación del sector privado debido a que, según el Reporte de Seguridad Cibernética e Infraestructura Crítica de las Américas, elaborado en 2015 por la OEA y la empresa *Trend Micro*, "más del 80% de la infraestructura que potencia el Internet y administra los servicios esenciales es propiedad del sector privado y es operada por este".

No obstante, aparecen muchas dudas sobre la forma más adecuada de canalizar constructivamente la participación de los actores señalados. Sin embargo, la experiencia de países como Canadá, EE.UU, Reino Unido, España y Alemania, entre otros, con años de experiencia en el tema puede servir como modelo. Asimismo, buenas prácticas asociadas a la promoción de la coordinación interagencial y la cooperación internacional constituyen aspecto de especial interés en el estudio de caso sobre ciberseguridad.

Lo descrito, permite establecer una serie de problemas, dilemas, desafíos y buenas prácticas que es necesario identificar, analizar y compartir con la finalidad de colaborar en la discusión sobre el nivel de ciberseguridad requerido y el existente para reducir la brecha detectada. Ello cobra especial relevancia cuando se tiene en consideración que un incidente en el ciberespacio tarde o temprano le ocurrirá a todo usuario de éste. La diferencia estará dada por el tiempo demorado en detectarlo, la capacidad para enfrentarlo y la resiliencia para superarlo.

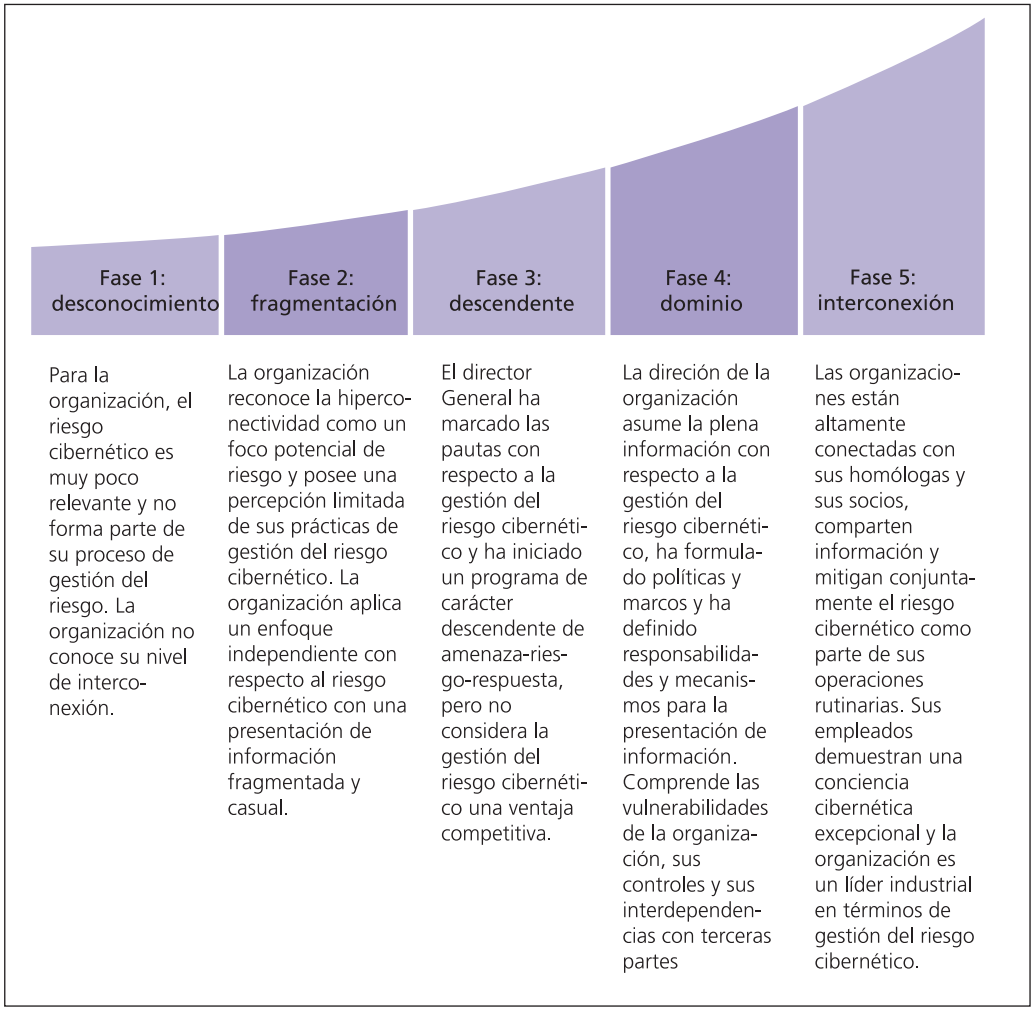
Por este motivo, la OEA, a través del *Comité interamericano contra el terrorismo* (CICTE), aborda los asuntos de Seguridad Cibernética. Ya en el año 2004, los Estados miembros aprobaron la "Estrategia interamericana integral para combatir las amenazas a la seguridad cibernética" en la resolución (AG/RES. 2004 XXXIV-O/04). Desde este organismo se "emplea un enfoque integral en la construcción de capacidades de seguridad cibernética entre los Estados miembros, reconociendo que la responsabilidad nacional y regional para la seguridad cibernética cae sobre una amplia gama de entidades tanto del sector público como el privado, los cuales trabajan en aspectos políticos y técnicos para asegurar el ciberespacio".

Destacan entre los objetivos que se han propuesto los siguientes:

El establecimiento de grupos nacionales de 'alerta, vigilancia y prevención', también conocidos como *equipos de respuesta a incidentes* (CSIRT) en cada país; crear una red de alerta Hemisférica que proporciona a formación técnica a personal que trabaja en la seguridad cibernética para los gobiernos de las Américas; promover el desarrollo de Estrategias Nacionales sobre Seguridad Cibernética; y fomentar el desarrollo de una cultura que permita el fortalecimiento de la Seguridad Cibernética en el Hemisferio (OEA y CICTE 2017).

Ilustra la orientación del trabajo a desarrollar, la XVI Declaración CICTE denominada "Fortalecimiento de la Cooperación y del Desarrollo en la Seguridad Cibernética y la Lucha contra el Terrorismo en las Américas", efectuada en el año 2016. Ello ha justificado la elaboración de un número especial sobre

Figura 4. Modelo de madurez organizacional



Fuente: Foro Económico Mundial (2012).

ciberseguridad. Artículos específicos sobre diversas aristas del tema expuesto buscan ilustrar tanto la complejidad como la diversidad del fenómeno. En este sentido, a continuación, el lector encontrará siete artículos que pueden ser clasificados en dos categorías: por un lado, sobre temas amplios queabordan aspectos de la ciberseguridad que pueden ser aplicados a diferentes situaciones, como es el caso de los ciberdelitos vinculados al ciberterrorismo y la ciberinteligencia; por otro lado, es posible encontrar materias que analizan casos específicos de seguridad en el ciberespacio en países específicos como Ecuador (gobernanza en ciberdefensa), Brasil (política de ciberseguridad), México (video vigilancia en puebla), Venezuela (cibervictimización) y Argentina (ciberdefensa y regulación legal). Se destaca en cada uno de los artículos, la rigurosidad para tratar temas novedosos en los cuales hay poca bibliografía disponible, por lo que constituyen un valioso aporte en la construcción de un acervo de conocimiento con estándares académicos en ciberseguridad.

En síntesis, el ciberespacio es un ambiente de creciente interacción social, que desde una perspectiva política tiende a ser reconocido como un bien público y desde la Defensa ha sido considerado una nueva dimensión o dominio de la guerra. La existencia de riesgos y amenazas obliga a considerar la ciberseguridad como una condición que debe ser provista por el Estado. Los países Latinoamericanos no están eximidos de abordar este tema desde una perspectiva de política pública con la finalidad de ofrecer (garantizar) crecientes niveles de seguridad. Organismos multilaterales como la OEA han elaborado documentos para apoyar a los países en la materia con la finalidad de ayudar a promover la existencia de organizaciones e institucionales que sean maduras desde una perspectiva de ciberseguridad, tal como se ilustra en la figura 4.

Bibliografía

Foro Económico Mundial. 2012. "Asociación por la Resiliencia Cibernética", http://www3.weforum.org/docs/WEF_IT_PartneringCyberResilience_Guidelines_2012_SP.pdf.

Karpesky. 2015. "Los riesgos futuros: protéjase", acceso el 5 de mayo de 2017, http://go.kaspersky.com/rs/802-IJN-240/images/APT_Report_ONLINE_AW_ES.pdf.

OEA (Organización de Estados Americanos) y CICTE (Comité Interamericano contra el Terrorismo). 2017. "Seguridad cibernética", https://www.sites.oas.org/cyber/Es/Paginas/default.aspx.

OEA (Organización de Estados Americanos) y Trend Micro. 2015. "Reporte de Seguridad Cibernética e Infraestructura Crítica de las Américas", https://www.sites.oas.org/cyber/Documents/2015%20-%20OEA%20Trend%20Micro%20Reporte%20Seguridad%20Cibernetica%20y%20Porteccion%20de%20la%20Inf%20Critica.pdf.

Sancho, Carolina. 2016. "Ciberespacio bien público mundial en tiempos de globalización: Política pública de ciberseguridad una necesidad imperiosa y la ciberdefensa como desafíos en el siglo XXI". Ponencia presentada en *XVII Conferencia de Directores de Colegios de Defesa Ibero*-americanos, Brasil, 3 y 7 de octubre.

Torres, Manuel. 2013. "Ciberguerra". En *Manual de Estudios Estratégicos y Seguridad In-*

ternacional, coordinado por Javier Jordán, 329-348. España: Plaza y Valdés.

UIT (Unión Internacional de Telecomunicaciones). 2014. "Medición de la Sociedad de la Información 2014. Resumen Ejecutivo", https://www.itu.int/en/ITU-D/Statistics/Documents/publications/mis2014/MIS_2014_Exec-sum-S.pdf.

_____. 2015. "Medición de la Sociedad de la Información 2015. Resumen Ejecutivo", https://www.itu.int/en/ITU-D/Statistics/Documents/publications/misr2015/MISR2015-ES-S.pdf.

_____. 2016. "Measuring the Information Society Report 2016. Key findings", acceso el 6 de mayo, http://www.itu.int/en/ITU-D/Statistics/Documents/publications/misr2016/MISR2016-KeyFindings.pdf.