Ataques Cibernéticos

¿Está preparada América Latina?*

Kaitlin Lavinder

América Latina está cada vez más en riesgo de ser el blanco de agresores cibernéticos. Tanto la cifra de ciudadanos, como la cifra de aquellos conectados a la *Internet* aumentan cada vez más. "Más del cincuenta por ciento de las personas están en línea, que es bastante grande comparado con otras regiones […] América Latina cuenta con una de las tasas de crecimiento más altas de usuarios de *Internet*", dijo Francesca Spidalieri, experta en seguridad cibernética en el Instituto Potomac para Estudios de Política y en el Centro Pell de la Universidad Salve Regina.[1] Frederic Lemieux, el cofundador de la Academia Cibernética de la George Washington University y un experto para la organización de noticias sobre seguridad nacional, *The Cipher Brief,* destaca que América Latina representa alrededor del diez por ciento de usuarios de *Internet* en el mundo, y la cantidad de usuarios ha aumentado un diecisiete por ciento desde 2013. "En el 2015, Brasil alcanzó más de 160 millones de usuarios de *Internet*, Chile cuenta con más de 15 millones y México ha llegado a más de 60 millones de usuarios", declaró Lemieux.[2]

Además, América Latina es el hogar de un número de economías en desarrollo, incluyendo las cuatro economías más grandes en la región: Brasil, México, Argentina y Colombia (en orden, comenzando con la más grande en términos de PIB). Esos países, a medida que crecen, se están tornando cada vez más tecnológicamente inteligentes. Además, algunas de las economías más pequeñas de América Latina, son sumamente innovadoras, y, por lo tanto, también se están tornando más tecnológicamente inteligentes. Entre ellas se encuentran Chile, Costa Rica, Perú y Uruguay. La Organización de Estados Americanos (OEA) y el

Una corta versión de este artículo originalmente apareció en thecipherbrief.com

Banco Interamericano de Desarrollo (BID) están trabajando arduamente con los países de América Latina para garantizar que la región cuenta con la protección cibernética adecuada (la OEA provee investigación y análisis extenso mientras que el BID ofrece recursos para ayudar a los países a crear sus propios equipos cibernéticos. Aun así, el coste de los delitos cibernéticos en América Latina y el Caribe (LAC, por sus siglas en inglés) es elevado, alrededor de US$90 mil millones por año —eso es alrededor del 15,65 por ciento del coste del delito cibernético a nivel mundial.[3] Un informe publicado por *Symantec,* un proveedor de productos y soluciones de seguridad, alega que el coste de los delitos cibernéticos ha alcanzado US$8 mil millones en Brasil, US$3 mil millones en México y US$464 millones en Colombia.[4]

No es sorprendente que las cuatro economías más grandes de América Latina también son las más vulnerables a los ataques cibernéticos. Por ejemplo, Brasil, Colombia y Argentina son las tres fuentes principales de ataques de *phishing* en LAC, explicando por el 74 por ciento de todos los ataques de *phishing* en América Latina y el 3,2 por ciento a nivel mundial, según el informe de *Symantec.*[5] Pablo Dubois, un gerente de productos de seguridad para Level 3 Communications (un proveedor de servicios de red global), dice que el 12 por ciento de los ataques Distribuidos de Denegación de Servicio (DDoS, por sus siglas en inglés) son dirigidos a América Latina, y que esa cifra está aumentando. "Nuestras investigaciones muestran, en orden, que Brasil, Argentina, México, Venezuela y Chile cuentan con la mayor cantidad de víctimas", dijo Dubois. Él explica, "Estos cinco países representan el 80 por ciento del total de víctimas C2 en América Latina. Los C2, los servidores de mando y control, son los cerebros de las operaciones maliciosas. Los C2 emiten instrucciones a las máquinas infectadas, las redes robot (*botnets),* para llevar a cabo el ataque".[6]

Chile es la sexta economía más grande en América Latina, después de Perú y antes que Venezuela y, por lo tanto, está bastante alta en la lista de amenazas cibernéticas. Además, Chile —junto con Costa Rica— consistentemente también están a la cabeza de las innovaciones en la región, incluyendo innovación en el sector tecnológico. Lourdes Casanova, quien trabajó en el proyecto InnovaLatino en el 2011 para identificar las áreas de innovación en América Latina, explica que esto es porque los ingresos per cápita en esos países se encuentran entre los más altos en la región, las oportunidades para una buena educación universitaria abundan, las inversiones del gobierno son altas y al sector privado le va bastante bien con respecto a la innovación. Lourdes, quien es la Directora del Instituto de Mercados Emergentes en la Cornell University, también destaca a Argentina como ser un "lugar bastante de moda para la tecnología".[7] El Líder Técnico Principal en la División de Competencia e Innovación del BID, Juan Carlos Navarro, hace eco de ello diciendo, "Argentina es un país donde los problemas de tecnología e innovación están en primera fila […] La consistencia y la calidad de la política pública y la dinámica del sector privado se han complementado muy bien entre sí".[8]

Perú y Uruguay también tienen el potencial de ser innovadores globales, según Cynthia Anderson, Directora del Programa Latinoamericano del Centro Wilson.[9] Por ejemplo, Perú ha presenciado un auge en la agricultura no tradicional —o sea, utilizando tecnología para desarrollar cultivos que nunca antes podían cosecharse en Perú— observa Navarro. Esto fue posible debido a una fuerte inversión por parte del sector privado y apoyo del sector público, observa Navarro.[10] Por supuesto, la innovación tecnológica —como la de Chile, Costa Rica, Perú y Uruguay— viene acompañada de un riesgo elevado de ataques cibernéticos y la necesidad de contar con infraestructuras robustas de seguridad cibernética.

La pregunta es, ¿acaso estos países que están en más riesgo en América Latina están preparados o se están preparando para compensar los costes de seguridad cibernética de poblaciones en crecimiento, mayores innovaciones y fortaleciendo economías? Miguel Porrúa, un especialista líder de gobierno electrónico (*e-government*) en el BID, le llama al nivel

de preparación en América Latina "preocupante".[11] Porrúa recientemente trabajó en un informe de seguridad para 2016, un esfuerzo de colaboración entre el BID, la OEA y el Centro Global de Capacidad para Seguridad Cibernética en la Universidad de Oxford, llamado *"Cybersecurity: Are We Ready in Latin America and the Caribbean?"* (Seguridad Cibernética: ¿Estamos Preparados en América Latina y el Caribe?) El informe reveló que mientras que cierto número de países latinoamericanos desconocen completamente o no están preparados para lidiar con los retos del panorama cibernético del siglo XXI, seis países tienen un nivel intermedio de preparación: Argentina, Brasil, Chile, Colombia, México y Uruguay.[12] Esos países o bien han adoptado una estrategia nacional sobre seguridad cibernética (Brasil y Colombia) o están trabajando en ello. Un grupo de eruditos de un grupo de expertos/una institución de educación superior, la Fundación Getúlio Vargas observa, "El conocimiento de la importancia de crear estrategias de seguridad cibernética está aumentando entre los países [en LAC]."[13]

De hecho, aunque Argentina carece de una estrategia oficial de seguridad nacional cibernética, hay un proyecto de estrategia esperando que el gobierno lo adopte. *El National Program for Critical Information Infrastructure and Cybersecurity* (Programa Nacional para la Infraestructura y Seguridad Cibernética de Información Crítica [ICIC, por sus siglas en inglés]), fundado en el 2011, trabajó con agencias gubernamentales, el sector privado e instituciones académicas para crear la estrategia.[14] Argentina cuenta con una historia relativamente larga con la seguridad cibernética, comparada con el resto de la región. Dubois, quien vive en Argentina, expresa, "En 1994, Argentina fue una de las primeras naciones en establecer un Grupo de Coordinación de Respuesta a Incidentes de Seguridad (CSIRT, por sus siglas en inglés)," mientras que muchos países latinoamericanos recién se encuentran en las etapas nacientes de los CSIRT desarrollados y Grupo de Respuesta ante Emergencias Cibernéticas (CERT, por sus siglas en inglés).[15] La mayoría de los países aún tienen que crear mecanismos de defensa progresistas.[16]

Sin embargo, Brasil y Colombia parecen estar adelantadas a los acontecimientos. Brasil recientemente difundió su Estrategia de Seguridad de la Información y las Comunicaciones de Seguridad Cibernética de la Administración Pública Federal. Mientras, las Fuerzas Armadas Brasileñas recientemente establecieron un Comando de Defensa Cibernética oficial y una Escuela Nacional de Defensa Cibernética, según el informe OEA-BID-Oxford.[17] Esto tiene sentido ya que Brasil es un blanco principal para los ataques cibernéticos, ya que cuenta con la economía más grande de la región y es un país que ha invertido enormemente en la tecnología para promover el crecimiento económico.

Colombia, al igual que Brasil, tiene una política nacional de seguridad cibernética y una estrategia exhaustiva de defensa cibernética. Diego Molano, ex ministro de Colombia de Tecnologías de Informática y Comunicaciones, dice que de toda América Latina, el país es el "número uno" en política cibernética. Él explica que la administración, el ejército, las fuerzas policiales y el sector privado se unieron para crear la estrategia nacional.[18] Además, en el informe OEA-BID-Oxford se expresa que, "El nivel de conciencia social en cuanto a la importancia de la seguridad y privacidad de la *Internet* y la confianza en los sistemas digitales del país ha crecido en gran medida, debido en parte a las campañas nacionales […] El desarrollo de la educación sobre la seguridad cibernética nacional también ha crecido notablemente".[19] Aun así, Molano opina que a la industria de la seguridad cibernética le falta algo. Sencillamente no hay suficientes personas que tienen la educación sobre la seguridad cibernética para crear una industria sólida que pueda proteger adecuadamente al país de los ataques cibernéticos, comentó.[20] El gobierno continúa trabajando sobre este aspecto.

Chile, aunque no ha emitido un plan nacional de seguridad cibernética como lo han hecho Brasil y Colombia, posee un marco legal exhaustivo para lidiar con los delitos cibernéticos y, según se menciona en el informe OEA-BID-Oxford, "la concienciación en las

instituciones gubernamentales es extensa". Por ejemplo, las Fuerzas Armadas de Chile comparten las responsabilidades de información y defensa cibernética (aunque no hay una estructura central de comando y control). Investigadores de la OEA, BID y Oxford sugieren que el reto principal de Chile para seguir adelante es fortalecer sus capacidades de responder a incidentes.[21]

México también necesita reforzar sus iniciativas de respuesta, según el informe, porque aunque "la policía tiene una extensa capacidad para la investigación, México aún está creando sus leyes sobre el delito cibernético, lo que dificulta procesar esos actos". Dicho esto, el país está elaborando en la actualidad su Estrategia Nacional para la Seguridad en la Información y una política de seguridad de información que coloca la defensa cibernética bajo la responsabilidad de las Fuerzas Armadas.[22]

Uruguay —un nuevo líder con una tasa de penetración en la Internet del 61 por ciento, inclusive si es solamente la decimocuarta economía más grande en América Latina— parece que está tomando la seguridad cibernética tan en serio como las naciones latinoamericanas más desarrolladas. "Uruguay es un líder regional en el desarrollo de *software* de seguridad y un mercado para nuevas tecnologías y seguros de seguridad cibernética", observan investigadores de la OEA, BID y Oxford. En el 2009, el gobierno uruguayo aprobó una ley que le exige a todas las agencias gubernamentales que elaboren políticas de seguridad cibernética. Además, la Política de Defensa Nacional de la nación incorpora la defensa cibernética.[23]

Por otra parte, Costa Rica y Perú —dos países que ocupan puestos de algo rango en términos de innovación y tecnología y, por ende, requieren sistemas de seguridad cibernética fuertes— están menos equipados. Casi el 50 por ciento de la población de Costa Rica está conectada a la *Internet*. Pero "las autoridades judiciales luchan por procesar casos de delitos cibernéticos, ya que una cantidad limitada de fiscales y jueces tienen la capacidad de crear y establecer casos relacionados con evidencias electrónicas […] Costa Rica no cuenta con una milicia permanente y la Fuerza Pública tiene estructuras y capacidades limitadas para crear una resistencia cibernética […] El conocimiento del público sobre la seguridad cibernética es generalmente bajo", se alega en el informe OEA-BID-Oxford.[24]

Perú, una nación con el 40 por ciento de sus ciudadanos conectados a la *Internet*, es una historia similar. El país es un centro de actividad digital y comercio electrónico. En el informe OEA-BID-Oxford se destaca que en el 2013 los incidentes cibernéticos aumentaron un 30 por ciento. No obstante, concluye el informe, "Mientras que la concienciación de las partes interesadas ha aumentado como resultado de iniciativas recientes, la ausencia de una estrategia y una cadena de mando definida continúa impidiendo el fortalecimiento de la seguridad cibernética del país. Las fuerzas armadas también cuentan con un nivel básico de capacidad para la defensa cibernética, pero no cuentan con una política de defensa cibernética […] Si bien los servicios de gobierno y comercio electrónico continúan expandiéndose en Perú, la concienciación sobre la seguridad cibernética de la sociedad es generalmente baja".[25]

No es ninguna sorpresa que, en general, los países con la mayoría de recursos (que a menudo se duplica como los que están más en riesgo de amenazas de seguridad cibernética) también son los que están más preparados para lidiar con los retos de un mundo digital cada vez mayor. De hecho, Spidalieri destaca que todos los países latinoamericanos cuentan con recursos limitados para lidiar con la seguridad cibernética, razón por la cual la región tiene la suerte de que la OEA y el BID estén trabajando tan arduamente en estas cuestiones y ofreciendo un foro para que los países se reúnan y discutan retos, oportunidades y soluciones.[26] Sin embargo, aún hay un problema con la falta de confianza, tanto entre los gobiernos y el sector privado como entre los gobiernos. Las asociaciones públicas y privadas (PPP, por sus siglas en inglés) son necesarias para crear adecuadamente regímenes de

seguridad cibernética, sin embargo aún están limitadas en muchos países latinoamericanos. Spidaliere, junto con Melissa Hathaway y Jennifer McArdle, expertas líderes en seguridad cibernética, explican, "La falta de confianza entre las partes interesadas, y la ausencia de centros de coordinación o intermediarios de información autorizados aún socavan la capacidad de la mayoría de los países en LAC de establecer mecanismos oficiales de intercambio de información".[27]

Un informe del 2015 de la OEA y de *Trend Micro* descubrió que solamente el 21 por ciento de los operadores de infraestructura crítica hablan con los gobiernos acerca de la resistencia cibernética de sus sistemas.[28] El editor del informe, Belisario Contreras, quien también es Gerente del Programa de Seguridad Cibernética de la OEA (y colaboró en el informe OEA-BID-Oxford) y un experto en *The Cipher Brief,* comenta, "A menudo las empresas se preocupan que revelarle al gobierno incidentes cibernéticos resultará en sanciones o una pérdida de confianza por parte de los consumidores".[29]

Lemieux, de la Academia Cibernética de la GWU, explica que la realidad geográfica de una región consta de tres regiones secundarias (América del Sur, América Central y el Caribe) podría traducirse en una cifra de retos complejos. Según Lemiuex:

> "El primero es el desequilibrio aplastante en términos de un nivel de sofisticación de la tecnología de la informática. Muchos países apenas están experimentando la revolución digital a causa de dificultades internas (conflictos, economías estancadas, pobreza generalizada, etc.). Un segundo reto está relacionado con la discrepancia de las regulaciones y las leyes de un país a otro, impactando cómo se define el delito cibernético (si es que se define) y cómo se debe hacer cumplir. Un tercer reto es el nivel de corrupción que azota a los países latinoamericanos, resultando en un déficit de confianza cuando se trata de cooperación entre las agencias. Otro reto importante es la cultura de la seguridad cibernética o "la inseguridad cibernética" que prevalece en los países latinoamericanos. Más precisamente, muy a menudo negocios pequeños y medianos y las agencias gubernamentales tienden a creer que nadie está realmente interesado en hacerles daño y, por lo tanto, invierten muy poco en programas preventivos o medidas proactivas".[30]

Porrúa, del BID, agrega que él no ve un espacio cibernético común a lo largo de América Latina en un futuro próximo. Es difícil para los países coordinar entre sí, agrega Porrúa, entonces coordinar entre sí es extremadamente difícil.[31] El ex Ministro Molano ofrece dos motivos para ello. Primero es que en cualquier sector —no solamente el de seguridad cibernética— es una tarea enorme para los gobiernos latinoamericanos colaborar a lo largo de los sectores. Cada vez que una entidad gubernamental tiene que trabajar con otra, o el sector público tiene que colaborar con el sector privado, hay muchos retos, explica Molano. La segunda explicación tiene que ver con el liderazgo dentro de los países. Los líderes se preocupan de la política y de permanecer en el poder y, por lo tanto, un tema como el de la seguridad cibernética puede que termine al final de sus listas de cosas que hacer.[32]

Al utilizar las pautas y la ayuda de la OEA, el BID y las partes interesadas públicas y privadas, América Latina tiene una oportunidad ahora mismo de crear una red de seguridad cibernética fuerte e integrada antes que los agresores se infiltren profundamente en la región. Las economías más grandes —Argentina, Brasil, Colombia y México— ya están en riesgo y están gastando miles de millones de dólares en combatir el delito cibernético. Las economías más innovadoras —Chile, Costa Rica, Perú y Uruguay— están en un riesgo cada vez mayor, pero en general cuentan con niveles de preparación menos desarrollados que los de las cuatro economías más grandes. Estaría en el mejor interés en general de la región enmendar cualquier falta de confianza y

trabajar juntos para protegerse en contra de una de las amenazas del siglo XXI más grandes y que crece cada vez más: los ataques cibernéticos. ❑

Notas

1. Francesca Spidalieri, entrevista de Kaitlin Lavinder, 23 de agosto de 2016.
2. Frederic Lemieux, "*The Problems with Response and Prevention*" (Los problemas con la respuesta y la prevención), *The Cipher Brief*, última modificación el 29 de abril de 2016, https://www.thecipherbrief.com/article/latin-america/problems-response-and-prevention-1092.
3. *Center for Strategic and International Security Studies* y McAfee, "*Net Losses: Estimating the Global Cost of Cybercrime*" (Pérdidas netas: Calculando el coste global del delito cibernético), junio de 2014, http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf.
4. Organización de Estados Americanos y Symantec, "*Latin American and Caribbean Cybersecurity Trends*" (Tendencias latinoamericanas y caribeñas sobre la seguridad cibernética), junio de 2014, http://www.symantec.com/content/en/us/enterprise/other_resources/b-cyber-security-trends-report-lamc.pdf.
5. Ibid.
6. Pablo Dubois, "*An Opportunity for Bad Actors*" (Una oportunidad para los actores malos), *The Cipher Brief*, última modificación, 29 de abril de 2016, https://www.thecipherbrief.com/article/latin-america/opportunity-bad-actors-1092.
7. Lourdes Casanova, entrevista de Kaitlin Lavinder, 17 de agosto de 2016.
8. Juan Carlos Navarro, entrevista de Kaitlin Lavinder, 18 de agosto de 2016.
9. Cynthia Arnson, "*Fostering Innovation Ecosystems in Latin America*" (Adoptando ecosistemas de innovación en América Latina), (presentación, The Wilson Center, Washington, DC, 2 de junio de 2016).
10. Juan Carlos Navarro, entrevista de Kaitlin Lavinder, 18 de agosto de 2016.
11. Miguel Porrúa, entrevista de Kaitlin Lavinder, 31 de agosto de 2016.
12. Banco Interamericano de Desarrollo y la Organización de Estados Americanos, "*Cybersecurity: Are We Ready in Latin America and the Caribbean?*" (Seguridad cibernética: ¿Estamos preparados en América Latina y el Caribe?), 2016,https://publications.iadb.org/handle/11319/7449?locale-attribute=en&locale-attribute=pt&locale-attribute=es&.
13. Fundación Getúlio Vargas, "*Cybersecurity, Privacy and Trust: Trends in Latin America and the Caribbean*" (Seguridad cibernética, privacidad y confianza: Tendencias en América Latina y el Caribe) en *Cybersecurity: Are We Ready in Latin America and the Caribbean?* 7.
14. "Argentina," en *Cybersecurity: Are We Ready in Latin America and the Caribbean?* 50.
15. Pablo Dubois, "*An Opportunity for Bad Actors*" (Una oportunidad para los actores malos), *The Cipher Brief*, última modificación el 29 de abril de 2016, https://www.thecipherbrief.com/article/latin-america/opportunity-bad-actors-1092.
16. Kaitlin Lavinder, "*Latin America: The New Frontier for Cyber Attacks*" (América Latina: La nueva frontera para ataques cibernéticos), *The Cipher Brief*, última modificación el 29 de abril de 2016, https://www.thecipherbrief.com/article/latin-america/latin-america-new-frontier-cyber-attacks-1092.
17. "Brasil," en *Cybersecurity: Are We Ready in Latin America and the Caribbean?* 60.
18. Diego Molano Vega, entrevista de Kaitlin Lavinder, 31 de agosto de 2016.
19. "Colombia," en *Cybersecurity: Are We Ready in Latin America and the Caribbean?* 64.
20. Diego Molano Vega, entrevista de Kaitlin Lavinder, 31 de agosto de 2016.
21. "Chile," en *Cybersecurity: Are We Ready in Latin America and the Caribbean?* 62.
22. "México," en *Cybersecurity: Are We Ready in Latin America and the Caribbean?* 88.
23. "Uruguay," en *Cybersecurity: Are We Ready in Latin America and the Caribbean?* 108.
24. "Costa Rica," en *Cybersecurity: Are We Ready in Latin America and the Caribbean?* 66.
25. "Perú," en *Cybersecurity: Are We Ready in Latin America and the Caribbean?* 96.
26. Francesca Spidalieri, entrevista de Kaitlin Lavinder, 23 de agosto de 2016.
27. Hathaway, McArdle y Francesca Spidalieri, "*Reflections on the Region*" (Reflexiones sobre la región), en *Cybersecurity: Are We Ready in Latin America and the Caribbean?* 115.
28. Organización de Estados Americanos *y Trend Micro*, "*Report on Cybersecurity and Critical Infrastructure in the Americas"* (Informe sobre la seguridad cibernética y la infraestructura crítica en las Américas), 2015, http://www.trendmicro.com/clooud-content/us/pdfs/security-intelligence/reports/critical-infrastructures-west-hemisphere.pdf.
29. Belisario Contreras, "*The Rising Cyber Threat*" (La amenaza cibernética en crecimiento), *The Cipher Brief*, última modificación el 26 de enero de 2016, https://www.thecipherbrief.com/article/rising-cyber-threat.
30. Frederick Lemieux, "*The Problems with Response and Prevention"* (Los problemas con la respuesta y la prevención), *The Cipher Brief,* última modificación el 26 de abril de 2016, https://www.thecipherbrief.com/article/latin-america/problems-response-and-prevention-1092.

31. Miguel Porrúa, entrevista de Kaitlin Lavinder, 31 de agosto de 2016.
32. Diego Molano Vega, entrevista de Kaitlin Lavinder, 31 de agosto de 2016.

Kaitlin Lavinder es una periodista de seguridad nacional en *The Cipher Brief* (https://www.thecipherbrief.com) cubriendo a Europa, África y América Latina. Anteriormente, se desempeñó como productora de noticias para el Canal de Noticias 8 en Washington, D.C., donde era responsable de los informes matutinos y segmentos de asuntos internacionales, POLITICO. También pasó un tiempo en la Embajada de Estados Unidos en Berlín trabajando en la Sección de Prensa. Lavinder obtuvo su Maestría de la Escuela Johns Hopkins de Estudios Internacionales Avanzados (SAIS) y su licenciatura en Radiodifusión, Telecomunicaciones y Medios de Comunicación de Temple University. Habla inglés y alemán y ha llevado a cabo investigaciones en Berlín, Varsovia, Gdansk, Londres y Tokyo.