¨Ciberseguridad en el Sector Bancario de América Latina y el Caribe¨
Simposio sobre Ciberseguridad en Las Américas.
Organización de Estados Americanos (OEA)
Washington, D.C., septiembre 2018

José Ml. López Valdés*

Introducción

Agradezco a los Sres. Luis Almagro, Secretario General y Belisario Contreras, Director del Programa de Ciberseguridad de la Organización de Estados Americanos OEA, por la invitación que nos hicieron para participar en esta importante reunión sobre Ciberseguridad en Las Américas.

En los últimos años, nuestras vidas en términos sociales, económicos y culturales, han sido transformadas por la tecnología. Estos desarrollos han revolucionado nuestra forma de realizar ciertas actividades cotidianas, aumentando la calidad de vida de las personas en todo el mundo[1].

Ciertamente, las nuevas tecnologías están impulsando industrias claves en los sectores de la salud, la educación, el comercio, la energía y el transporte. Tal es el impacto de los avances tecnológicos que el Banco Interamericano Desarrollo (BID) plantea en una publicación reciente, que la llamada "Revolución Digital" o "Cuarta Revolución Industrial" superará a las anteriores en cuanto a escala, alcance y complejidad[2]. A su vez señala que para 2017, la economía digital tenía un valor ascendente a US$11.5 billones equivalente al 15.5% del PIB mundial, estimándose

*Reconoce el aporte y la contribución a esta presentación del Sr. Julio Lozano, Director de Estudios Económicos de la Asociación de Bancos Comerciales de la República Dominicana Inc. (ABA)

[1] Pofuk, Tin. (2014). *"Human capital and developing economies: Benefits and solutions for policy-makers".* University of Primorska, Faculty of Management, Slovenia.

[2] Banco Interamericano de Desarrollo (2018). "*Disrupción Exponencial en la Economía Digital". III* Cumbre Empresarial de las Américas, Perú 2018.

que para 2025 la misma alcanzaría los US$23.0 billones, equivalente al 24% del PIB mundial.

El sistema financiero no ha escapado a las tendencias de "la Revolución Digital". En particular, los bancos se están transformando con el objetivo de convertirse en "bancos digitales", adaptándose a las nuevas demandas de los consumidores en un contexto en el que se estima que en unos pocos años el 75% de ellos pertenecerán a la generación "millenial", definidas como aquellas personas que se valen de la tecnología para llevar a cabo gran parte de sus actividades cotidianas[3].

Como parte de su transformación digital, los bancos están desarrollado una serie de productos y servicios financieros que reducen el costo de las transacciones, haciéndolas más rápidas y eficientes, con lo cual los clientes ahorran tiempo y dinero, lo que contribuye a elevar la calidad de vida y los niveles de productividad laboral, aportando nuevos beneficios para la sociedad.

La tecnología permite a las entidades financieras operar con menores costos operativos y mayor eficiencia, resultando esto en una mayor capacidad para desarrollar canales alternativos que permiten "acercar el banco a las personas", sobre todo, a aquellas no bancarizadas, elevando los niveles de inclusión financiera en nuestros países[4].

No obstante estos beneficios, el uso de la tecnología representa también, tanto para la banca mundial como latinoamericana, una amenaza en términos de la gestión de seguridad. Los bancos históricamente han lidiado con la seguridad de sus clientes en las sucursales, con la falsificación de cheques y otros instrumentos financieros, con el resguardo de la información física y con la violencia criminal. Ahora, en la era de la "banca digital", los delincuentes dirigen sus esfuerzos hacia

[3] https://www.forbes.com.mx/6-rasgos-clave-de-los-millennials-los-nuevos-consumidores/
[4] Karp, Nathaniel. (2015). *"Technology, Opportunity & Access: Understanding Financial Inclusion in the U.S."* Fuente: https://www.bbvaresearch.com/wp-content/uploads/2015/07/WP15-25_FinancialInclusion_MSA.pdf

el campo virtual, modernizando sus métodos y organizándose mejor, con el objetivo de encontrar vulnerabilidades en los sistemas informáticos de los bancos.

Costo de los Ataques Cibernéticos

En general, los delitos cibernéticos han proliferado en todos los sectores de la economía. Sin embargo, los bancos e instituciones financieras tienden a ser el blanco preferido de los cibercriminales. Así, en 2017, según reportes de IBM Security, con un 27% del total, la industria de servicios financieros se posicionó como el sector con mayor cantidad de ataques cibernéticos[5] por delante del gobierno y las empresas de telecomunicaciones.

Por otra parte el Foro Económico Mundial estima las pérdidas económicas producidas en América Latina por los ataques cibernéticos en US$87,940 millones[6], aproximadamente un 1.6% del PIB regional, en 2017, siendo Brasil, México Venezuela y Argentina los países más afectados. Asimismo, el Informe Anual de Ciberseguridad CISCO 2018 encuentra que más de la mitad de los ataques tienen un costo que sobrepasa los US%500 mil[7]. Además, la región experimentó 70 millones de ciberataques durante la primera mitad de 2017 y un 66% de las organizaciones financieras enfrentaron al menos un ataque en los últimos 24 meses[8].

Ahora bien, más allá de las pérdidas monetarias, la realidad es que para cualquier institución es difícil cuantificar el verdadero costo de un ciberataque. El impacto no solo es económico, sino que también intervienen otros elementos tales como el daño a la reputación y confianza del público, factores que representan potenciales pérdidas de clientes y negocios, por lo que el verdadero costo de los ciberataques termina siendo aún mayor.

---

[5] González, Adrián. (31 de julio, 2018). ¿Cómo avanza la ciberseguridad en la banca? Publicado en https://revistaitnow.com/como-avanza-la-ciberseguridad-en-la-banca/

[6] Idem 5.

[7] https://www.netec.com/single-post/Informe-Anual-de-Ciberseguridad-Cisco-2018

[8] Núñez, Claudio. Ciberseguridad y administración del riesgo en bancos y empresas de servicios financieros. Fortinet (2018).

Importancia de la Ciberseguridad

En virtud de lo anterior, en el mundo empresarial y también en los gobiernos a nivel global, ha crecido la conciencia acerca de la necesidad de una estrategia de ciberseguridad, entendiéndose esta como el conjunto de herramientas, políticas, procesos, personal y tecnologías que las organizaciones utilizan para proteger sus activos y a sus usuarios. Así, la última encuesta de seguridad global de Ernst & Young reveló que el 59% de las grandes empresas encuestadas, aumentó su presupuesto de ciberseguridad con respecto al año anterior[9].

En ese contexto, es importante señalar que el sector bancario ha adoptado una postura cada vez más proactiva. Las inversiones en este frente crecen acorde a la problemática en cuestión. A nivel global, por ejemplo, JP MORGAN anunció un incremento de US$250 millones en su presupuesto de ciberseguridad, para llevarlo a US$500 millones[10]. Por su lado, Bank of América anunció que la ciberseguridad sería la única área sin restricciones presupuestarias[11]. A nivel latinoamericano, en el Congreso Latinoamericano de Automatización Bancaria 2017 (CLAB), organizado por FELABAN, se reveló que la banca regional ha incrementado las inversiones en seguridad desde un 7% hasta un 10% de los presupuestos de tecnología.

Amenazas en Ciberseguridad

De esta forma, el sector empresarial y bancario busca hacerle frente a múltiples formas de delincuencia cibernética. En este sentido, los análisis de las más importantes compañías de seguridad cibernética han identificado al menos 18 amenazas[12] que requieren especial atención y una adecuada estrategia de respuesta por parte de las instituciones. Entre estas, por mencionar algunas s

[9] Ernts & Young. "Recuperando la ciberseguridad: Preparándose para enfrentar los ciberataques". 20va Encuesta Global de la Seguridad de la Información 2017-2018. https://www.ey.com/Publication/vwLUAssets/GISS_report_2017/$FILE/REPORT%20-%20EY%20GISS%20Survey%202017-18.pdf

[10] https://www.forbes.com/sites/stevemorgan/2016/01/27/bank-of-americas-unlimited-cybersecurity-budget-sums-up-spending-plans-in-a-war-against-hackers/#18dfe954264c

[11] Idem 9.

[12] https://bitlifemedia.com/2017/12/18-tendencias-ciberseguridad-2018/

encuentran entre otras, el Ransomware, el Internet de las Cosas, las Criptomonedas, el Robo de Datos Personales, Malwareless, la Nube, Noticias Falsas y el Phishing.

Por otro lado, aún si los sistemas de seguridad han logrado identificar gran parte de las formas de ciberdelincuencia, eso no quiere decir que el trabajo está terminado debido a que existen sistemas que no están preparados para aquellos sucesos que no han previsto, altamente improbables y que tienen un gran impacto que solamente puede analizarse "a posteriori". Por esta razón, debido a que los ciberriesgos siempre serán una constante, los bancos deben estar siempre actualizando sus modelos de gestión del riesgo.

Respuestas de los Bancos y de FELABAN

Afortunadamente en nuestra región los bancos están enfrentando decididamente la problemática, si bien cada uno lo hace con distintas estrategias y a distintas velocidades, lo cierto es que la gran mayoría es consiente que la transformación hacia una "banca digital" no puede darse de forma exitosa sin una estrategia integral de ciberseguridad.

El sector bancario latinoamericano actualmente trabaja diseñando y aplicando estrategias que involucran a todas las áreas relacionadas con la identificación, medición, priorización y respuesta a los ciberriesgos. Esto debe ser así porque los bancos entienden que la ciberseguridad es más que tecnología, involucra también procesos, análisis, personal capacitado y comprometido, pero sobre todo visión desde la alta gerencia de las instituciones bancarias.

En concreto, las estrategias más exitosas implican, en la mayoría de los casos, las siguientes acciones: equipos de respuesta multidisciplinarios integrados por miembros de la banca y de organismos de seguridad del Estado, con la responsabilidad de responder a las distintas áreas ciberdelincuenciales, recibiendo, revisando, analizando y sobre todo actuando de forma rápida y contundente ante todo reporte sobre riesgos a la seguridad cibernética.

Así, los equipos bancarios poco a poco migran hacia un modelo de "vigilancia digital" el cual consiste en la aplicación de las últimas tecnologías como el "machine learning" y la "inteligencia artificial" con el objetivo de aprender a detectar automáticamente patrones inusuales en el entorno cibernético. En la medida que los equipos de respuesta vayan perfeccionando el uso de estas herramientas, se fortalecerán las barreras defensivas del sistema bancario contra los crímenes cibernéticos.

Adicionalmente, el uso de la Nube como mecanismos de seguridad para proteger los datos es cada vez más frecuente entre los profesionales de seguridad. De esta forma, el Informe Anual de Ciberseguridad de CISCO 2018[13] indica que el 57% de los encuestados está alojando su información en la Nube en procura de una mayor seguridad de sus datos. No obstante lo anterior, es necesario mencionar que los delincuentes están constantemente buscando vulnerar la Nube. Por tal motivo, el uso de esta herramienta debe ser protegida mediante las mejores prácticas de seguridad como la "vigilancia digital" permanente y otras plataformas de seguridad.

En el contexto de América Latina, de acuerdo al Comité Latinoamericano de Seguridad Bancaria de FELABAN, los principales riesgos informáticos que se presentan en la banca son la clonación de tarjetas de crédito y débito, la suplantación de identidad en compras no presenciales y el "phishing". Sin embargo, para esta fecha ya existen importantes avances en esta materia, incorporándose la tecnología chip en las tarjetas de débito y crédito y el uso del "token" de seguridad en las compras online y para las consultas de las cuentas bancarias personales.

Por su parte, FELABAN contempla en su plan estratégico el desarrollo de actividades ligadas a las nuevas tendencias en tecnología y medios de pago. En este sentido, FELABAN apoya a la banca latinoamericana mediante la formación de los recursos humanos en temas de banca digital y ciberseguridad, mediante la

[13] Idem 7.

realización del **Diplomado en Prevención de Riesgos Integrales en la Seguridad Bancaria**, con una duración de un año y que se imparte en países de América Latina en coordinación con una universidad local, constituye uno de los pilares con los que contribuye a enfrentar la ciberdelincuencia en la región.

Concomitantemente con lo anterior, en las agendas académicas de todos los congresos que anualmente celebra FELABAN se incluyen temas relacionados con la transformación digital, la delincuencia tecnológica y la ciberseguridad. Al mismo tiempo, FELABAN ha creado una comunidad virtual en la web que incluyen una base actualizada de artículos, documentos, iniciativas y buenas prácticas sobre estos temas disponible para consulta online. Y recientemente la institución está llevando a cabo un proyecto de investigación con la cooperación de la Corporación Andina de Fomento (CAF) y Asociación Nacional de Instituciones Financieras (ANIF) sobre el Nivel de Madurez Digital en Sector Financiero Latinoamericano, que será dado a conocer durante la 52 Asamblea Anual de FELABAN, que se celebrará en República Dominicana a mediados de noviembre del año en curso.

No obstante los mencionados avances, el trabajo debe continuar, tal como afirma Dmitry Bestuzhev, Director del Equipo de Investigación y Análisis para Latinoamérica en Kaspersky Lab: "la seguridad de un banco no es una estrategia estática, sino que necesita evolucionar y adaptarse constantemente, basándose en la inteligencia obtenida sobre las tendencias, las nuevas amenazas y las técnicas de seguridad más recientes para mantener verdaderamente segura sus redes"[14].

Ahora bien, como ha señalado FELABAN[15], paralelo a los esfuerzos de la banca regional, **la colaboración entre bancos y el sector público es determinante para mitigar los riesgos cibernéticos de una forma más efectiva**. En particular, se resalta la **proactividad de gobiernos y reguladores** regionales en abordar esta problemática, trabajando junto a los bancos **para producir regulaciones tendentes**

[14] https://www.eltiempo.com/tecnosfera/novedades-tecnologia/tendencias-en-ciberseguridad-en-el-sector-financiero-85912

[15] Ciberseguridad: una prioridad para el sector bancario. Documentos FELABAN no.9, 11 de abril 2018.FELABAN

a la protección de datos, informaciones de los clientes y de cuentas bancarias, entre otras. Concomitantemente y debido a que los delincuentes no conocen fronteras, trabajan con recursos cuantiosos y continúan organizándose, **el combate integral contra ellos requiere por tanto de la cooperación internacional**. **Un solo país, un solo banco o un solo gobierno es incapaz de ganar esta batalla por sí solo**. **En FELABAN encontrarán siempre un aliado, para fortalecer el diálogo, para tender puentes entre todos los actores involucrados, con el objetivo común de brindar un entorno de máxima seguridad a los usuarios del sistema bancario en todo el hemisferio.**

18 Septiembre 2018.