Palabras del Secretario General de FELABAN Giorgio Trettenero Castro en la apertura del XXXIII Congreso Latinoamericano CELAES

29 Octubre de 2018

Miami, Florida, Estados Unidos

Sr. David Schwartz CEO FIBA

Sr. Santiago Rodriguez Presidente del Comité Latinoamericano Seguridad Bancaria

Señores Gobernadores de FELABAN, miembros del comité técnico latinoamericano de seguridad Bancaria, Señores profesionales de la seguridad Bancaria, Patrocinadores, amigos todos.

Como siempre quiero expresar la inmensa gratitud con todos aquellos amigos, colegas, trabajadores y directivos que nos han prestado su concurso y trabajo esmerado para que esta reunión llegue a su fase final. Agradeciendo a todo el equipo FIBA de Miami, a los integrantes del Comité Técnico de CELAES, y su junta directiva y por supuesto al equipo de FELABAN.

Gran parte del foco que la banca ha definido para estos años, ha sido trabajar en temas como: la regulación y supervisión especialmente en la que se refiere a los acuerdos del Comité de Supervisión Bancaria de Basilea, principalmente en la aplicabilidad de la proporcionalidad, pidiendo que antes de ejecutarla, tengamos estudios de impacto de las normas en los balances bancarios. Igualmente, trabajamos los temas de educación e inclusión financiera como

un derrotero transversal sobre la necesidad de que cada vez más grupos de la población tengan acceso a los servicios financieros prestados por entidades profesionales. De la misma forma hacemos gestiones por atender el fenómeno del De Risking y mantener los puentes con los supervisores en búsqueda de soluciones a este flagelo. Igualmente, venimos apoyando a la banca la importante necesidad del proceso de la transformación digital integral que las entidades bancarias y financieras requieren para redefinir su modelo de negocio en lo relacionado a la prestación de servicios financieros. En ese sentido consideramos que la seguridad digital es tema que se posiciona como una prioridad para nuestra gestión para apoyar este proceso de trasformación digital. Proteger los recursos del público, generar confianza, mantener el poder

adquisitivo de los fondos, es una de nuestras tareas históricas. Las mismas no han cambiado en su esencia, pero los medios y los modos son cambiantes.

Ante la inminente ola de cambios que se presenta, sabemos que el canal más importante que la banca tiene en la región es el que se relaciona con los mecanismos digitales que utilizan fundamentalmente la telefonía móvil como medio.

De acuerdo con el IV Reporte de Inclusión Financiera de FELABAN, mientras que en el año 2011 el canal de banca móvil era del 0.1% del total del número de operaciones de la banca, en el año 2017 el mismo representó el 38% del total. Este se comporta como el más dinámico en los últimos años al crecer a tasas promedio del 30% anual.

Los canales digitales, el uso del teléfono móvil, la inmediatez, la impaciencia del cliente y los consabidos cambios internos que una organización financiera debe realizar para responder a velocidades que hasta hace muy poco no imaginábamos.

En este nuevo océano de posibilidades la labor de los especialistas de seguridad ha cambiado. Hoy ya no nos preocupamos tanto por la seguridad física. Nuestra preocupación viene más del mundo informático. La nube, los servidores, los lenguajes de programación, el internet, las aplicaciones y todo lo que esto conlleva, se han convertido en la fuente de acciones y estudio de prevención. Todo esto para cumplir con la misión que la sociedad nos

encomienda. Cuidar los recursos líquidos de la economía que están en el sector financiero.

Las amenazas virtuales son una realidad, nos hacen daño, afectan nuestra reputación, generan costos y dejan un nefasto efecto psicológico al enfrentar un enemigo sin rostro.

Hoy por hoy, los temores entre las personas de negocios no se centran en las amenazas que todos tradicionalmente conocemos. En los Estados Unidos una encuesta[1] entre ejecutivos empresariales sobre los riesgos para los negocios, los ciberataques aparecen en primer lugar para el año 2018. Esto superando temas tan delicados y sensibles como lo son las crisis fiscales, las burbujas de precios financieros, y los ataques terroristas entre muchos otros.

[1] https://www.weforum.org/agenda/2018/01/our-exposure-to-cyberattacks-is-growing-we-need-to-become-cyber-risk-ready/

Los costos están lejos de ser despreciables. El World Economic Forum, que estima las pérdidas económicas producidas en América Latina por los ataques cibernéticos alcanzan US$87 mil millones[2], aproximadamente un 1.6% del PIB regional, en 2017, siendo Brasil, México Venezuela y Argentina los países más afectados.

La sofisticación y poder de estos nuevos criminales virtuales es de dimensiones titánicas. De acuerdo a un informe de Verizon en el año 2017, se informó que el 70% de los asaltos informáticos (*hackeos*) a nivel mundial fue descubierto 1 mes después de su ocurrencia. Este hallazgo concuerda con aquél del anterior

[2] ¿Cómo avanza la ciberseguridad en la banca? Disponible en https://revistaitnow.com/como-avanza-laciberseguridad-en-la-banca/

CEO de Cisco Systems, Jhon Chambers, quien afirmó en un sentido similar que "*Hay dos tipos de empresas: aquellas que han sido hackeadas, y aquellas que aún no saben que han sido hackeadas*"[3].

Este panorama nos recuerda que lo digital por supuesto cambia la perspectiva de los negocios, pero este nuevo horizonte, da lugar de manera inherente a nuevos riesgos. Pero para la banca esto no es una novedad. Nuestro trabajo es administrar y mitigar riesgos financieros y económicos.

Nuestros países vienen trabajando estratégicamente para adelantar acciones no solo de respuesta, sino de prevención. El sector

[3] ¿What does the Internet of Everything mean for security? Disponible en https://www.weforum.org/agenda/2015/01/companies-fighting-cyber-crime/

bancario y el sector financiero en general vienen adelantando acciones privadas. Pero por supuesto que no es una labor que podamos adelantar solos. La cooperación con otros sectores de la economía, con las instituciones del estado y con las autoridades de seguridad, defensa y policía. No en vano muchos departamentos de defensa nacional o entidades de inteligencia policial cuentan hoy en día con una división informática donde se lucha contra el ciberdelito, el fraude y tantas formas nocivas de crimen que han venido proliferando en el mundo digital en los últimos años.

Por su parte, FELABAN apoya a la banca latinoamericana mediante la formación de los recursos humanos en temas de banca digital y ciberseguridad, mediante la realización del Diplomado en Prevención de Riesgos Integrales

en la Seguridad Bancaria, 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.

Y para terminar, quiero resaltar que la ciberseguridad va más allá del tema tecnológico, involucra procesos, procedimientos, personal capacitado, presupuestos definidos, y sobre todo, visión de la más alta gerencia de las instituciones bancarias para coordinar una estrategia integral de ciberseguridad, con los presupuestos necesarios y suficientes, con la debida dotación de recursos humanos, técnicos y financieros y con líderes definidos como responsables de la seguridad integral.

Señores y señoras, lo he sostenido y lo repito con ustedes. Un solo banco, un solo supervisor o un solo gobierno, serán incapaces de ganar esta batalla si deciden hacerlo en forma aislada, esto se logra con equipos de ciberseguridad mas mecanismos de información y apoyo colaborativo y trabajo conjunto entre sector público y privado.

En FELABAN encontrarán siempre un aliado para fortalecer el diálogo y 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.

¡Muchas Gracias!