Mauricio Andrés Burgos Navarrete
Director en Universidad Autónoma de Chile (Temuco)

Ciberseguridad Bancaria en el Mercado Financiero de Chile

Economía, 08/09/2019

La ciberseguridad debe constituir un foco de atención relevante para distintos actores en el sistema financiero de Chile, máxime si se contempla que las debilidades que puedan existir afectarán en distintos grados a las partes involucradas en una transacción.

La ciberseguridad, independiente del contexto que se considere, se ha tomado la agenda de lo público y lo privado. Así tanto a nivel de gobierno como de gremios han estado procurando espacios para trabajo, análisis y definición de medidas que permitan prevenir y salvaguardar la integridad de los datos e información relevante. Situaciones en el último tiempo como los ataques de hackers a entes ligados a redes sociales, y otras en un nivel algo menor en el país, a unas compañías de seguros y bancos, pero no por ello sin importancia, han puesto el dedo en lo que hasta ese minuto se debe haber calificado perfecto: la seguridad en tiempos de tecnología digital.

De este modo, no es raro que la Asociación de Bancos e Instituciones Financieras (ABIF) su informe N° 139/2019 lo haya titulado Ciberseguridad en la Banca, concentrándose en tres aspectos, la tasa de fraude en el sector a nivel internacional, las iniciativas de la industria en materia de mitigación, y las amenazas cibernéticas y su impacto en Chile, de lo que destaca:

1° El papel del sector bancario y su esfuerzo expresado en un bajo porcentaje de fraude, lo que se evidencia acorde a Visa, en transacciones con tarjetas bancarias que la ubican a un tercio de la media mundial. Además, respecto a las transferencias electrónicas de fondos, si bien no hay datos abundantes y metódicos, al tomar como referencia el Reino Unido, se ubica a un tercio de valor.

2° Asimismo, se resalta la creación del Grupo de Coordinación de Ciberseguridad de la ABIF, ente por el cual los partícipes comparten información y prácticas, destacando: i) pinpass, que busca reducir el riesgo de uso ilícito de tarjeta, ii) perturbador magnético, que refuerza la protección ante la clonación y sustracción de datos de las tarjetas, iii) mensajería a clientes, que perfecciona el seguimiento oportuno de transacciones de los de usuarios, iv) monitoreo y prevención de fraudes, lo que

refuerza el resguardo en el uso de productos bancarios, v) uso de algoritmos más eficientes en el descubrimiento de fraudes, vi) autenticación vía biometría, vii) uso en tarjetas del estándar de chip EMV, y viii) campañas al público en temas de ciberseguridad.

3° El país está entre los más atacados globalmente, y según Kaspersky, se ubica en el lugar 14 de 188. A esto se suma que está en 2° lugar de los países más atacados que componen la OCDE, y 3° en Latinoamérica. En tanto, por el lado de usuarios, la empresa antes mencionada, expresa que el 0,8% ha sido atacado por programas maliciosos que buscan robar dinero, o bien, acceder a las cuentas bancarias, lo que nos ubica como 5° país OCDE más atacado y 8° en Latinoamérica.

Así, aun cuando las entidades bancarias han mostrado avances, en otros aspectos es preciso continuar por el sendero de la mejora continua, y muestra de aquello, por ejemplo, son aclarar en el panorama nacional cómo se resolverá finalmente el proyecto sobre Ciberseguridad Financiera, qué determinación se tomará respecto de la devolución de dineros sustraídos en fraudes a tarjetahabientes. Asimismo, es importante recordar que la tecnología avanza a una velocidad muy intensa, a lo cual con la misma fuerza le siguen los delitos y nuevas formas de ejecución de fraudes, y mucho más atrás suele ubicarse la reacción de prevención y el ajuste o modificación a los marcos legales existentes, piénsese en el caso de las Fintech.

Por ello, las instituciones y gremios deben seguir estudiando y analizando lo que sucede en otras latitudes proactivamente, en el ánimo de mitigar y/o frenar nuevas posibilidades de defraudación, las que pueden provenir del medio externo como interno, provocando impactos monetarios, así como no monetarios, tales como lo reputacional. En tal sentido, la educación financiera tiene mucho que aportar, instalando una cultura preventiva, la que no se puede considerar como responsabilidad de una sola parte. En consecuencia, debe mantenerse un estado de alerta y de ocupación. Y como bien señalan en el informe: “la ciberseguridad depende de todos y resguardarla es una responsabilidad compartida”.