DESAFÍOS DEL RIESGO CIBERNÉTICO EN EL SECTOR FINANCIERO PARA COLOMBIA Y AMÉRICA LATINA

ASOBANCARIA
Construyendo la **Confianza** y **Solidez** del sector financiero

OEA
Más derechos para más gente

DESAFÍOS DEL RIESGO CIBERNÉTICO EN EL SECTOR FINANCIERO PARA COLOMBIA Y AMÉRICA LATINA

DESAFÍOS DEL RIESGO CIBERNÉTICO EN EL SECTOR FINANCIERO PARA COLOMBIA Y AMÉRICA LATINA

DESAFÍOS DEL RIESGO CIBERNÉTICO EN EL SECTOR FINANCIERO PARA COLOMBIA Y AMÉRICA LATINA

CRÉDITOS

Luis Almagro
Secretario General

Farah Diva Urrutia
Secretaria de Seguridad Multidimensional

Alison August Treppel
Secretaria Ejecutiva
Comité Interamericano conrta el Terrorismo

Equipo Técnico de la OEA
Belisario Contreras
Barbara Marchiori de Assis
Kerry-Ann Barrett
Miguel Angel Cañada
David Moreno
Mariana Cardona
Diego Subero
Jaime Fuentes
Geraldine Vivanco

Santiago Castro Gómez
Presidente

Alejandro Vera Sandoval
Vicepresidente Técnico

Jaime Andrés Rincón Arteaga
Director de Gestión Operativa y Seguridad

Andrés Quijano Diaz
Profesional Senior

María Camila Barrera Neira
Profesional Junior

Santiago Castiblanco Hernandez
Profesional Junior

Primera edición, octubre de 2019

DESAFÍOS DEL RIESGO CIBERNÉTICO EN EL SECTOR FINANCIERO PARA COLOMBIA Y AMÉRICA LATINA

TABLA DE CONTENIDO

PRÓLOGO
OEA

LUIS ALMAGRO

Secretario General

Organización de los Estados Americanos (OEA)

Internet ha revolucionado el mundo que nos rodea y la forma en que interactuamos con los demás. Esto es particularmente cierto en América Latina y el Caribe, ya que casi 70% de la población está en línea y la tasa de crecimiento de usuarios de Internet es la tercera más altas del mundo – es decir, 2,4% entre 2000-2019.[1] En las Américas y el Caribe, se utiliza Internet para relacionarse con las personas, compartir ideas, gestionar negocios y realizar transacciones. Por todo ello, el sector financiero fue uno de los primeros en adoptar las tecnologías y ofrecerlas a sus clientes.

El sector financiero ha experimentado uno de los mayores índices de digitalización en los últimos años. Cada día un mayor número de clientes usan medios no presenciales para realizar transacciones por internet, pagos a través de dispositivos móviles o cualquier otro tipo de trámites bancarios. En Colombia, se estima que la población bancarizada dentro del universo de internautas es de 81%, y que 79,4% de la población bancarizada internauta ha consultado o hecho operaciones bancarias en línea en 2018.[2]

Por eso, los bancos también son pioneros en la adopción de medidas para asegurar la protección de sus clientes. De hecho, el sector financiero es tradicionalmente uno de los principales blancos de las amenazas cibernéticas. De acuerdo con el estudio de la OEA "El Estado de la Ciberseguridad en el Sector Bancario en América Latina y el Caribe," publicado en octubre de 2018, el 92% de las entidades bancarias identificaron algún tipo de evento (ataques exitosos y no exitosos) de seguridad digital, y el 37% de entidades bancarias manifestaron que sí fueron víctimas de ataques exitosos. La principal motivación de dichos ataques durante el año 2017 fueron motivos económicos (79% de las entidades bancarias víctimas).

En este contexto, la Secretaría General de la Organización de los Estados Americanos a través del Programa de Ciberseguridad adscrito al Comité Interamericano contra el Terrorismo (CICTE), en alianza con la Asociación Bancaria y de Entidades Financieras de Colombia (ASOBANCARIA), ha coordinado la publicación de este primer libro en la región que reúne artículos de expertos internacionales sobre la gestión del riesgo y de medidas de seguridad para la protección del sector financiero a nivel nacional en Colombia y también con impacto en toda América Latina.

Desde hace 15 años, la OEA ha estado comprometida con la protección de ciudadanos, empresas y gobiernos en el ciberespacio, apoyando a los Estados Miembros en el fortalecimiento de sus capacidades

en ciberseguridad. En 2004, los Estados Miembros de la OEA aprobaron la Estrategia Interamericana Integral para Combatir las Amenazas a la Seguridad Cibernética, que instaba a los países a coordinar esfuerzos con las múltiples partes interesadas en la lucha contra las amenazas cibernéticas en el hemisferio y proporcionaba un marco inicial para guiar tal enfoque. Esta visión colaborativa ha guiado el trabajo del Programa de Ciberseguridad de la OEA/CICTE junto a uno de los principales gremios de la región, como es ASOBANCARIA, para señalar la importancia de la ciberseguridad, remarcando a través de esta colaboración que la seguridad digital no es un asunto exclusivo de la agenda de los gobiernos, sino también de todas las partes implicadas. Los diferentes actores – sea a nivel local, nacional o internacional – tienen un papel que desempeñar en la lucha contra las amenazas cibernéticas.

Para la Secretaría General de la OEA es un gran honor apoyar una vez más a Colombia, con la colaboración de ASOBANCARIA, en un proyecto que busca aumentar la conciencia sobre la importancia de la seguridad digital. Colombia fue el primer país de la región en desarrollar una estrategia nacional de ciberseguridad en 2011, así como el primer país en revisarla con un enfoque integral y colaborativo, fomentando la gestión del riesgo y la participación de las múltiples partes interesadas. Fue también Colombia el primer país en llevar a cabo un estudio sobre el impacto de incidentes de seguridad digital en las organizaciones colombianas con el apoyo del Programa de Ciberseguridad de la OEA/CICTE.

Igualmente, Colombia será el segundo país de la región – después de México – en publicar un estudio completo sobre el estado de la ciberseguridad en el sector financiero de la mano de nuestra organización. Son notables los esfuerzos llevados a cabo por las entidades financieras colombianas para garantizar la seguridad digital en las transacciones de sus clientes. Por ejemplo, ASOBANCARIA ha liderado la creación del CSIRT Financiero, un centro de respuesta a incidentes cibernéticos que brinda apoyo al sistema financiero, y que es el resultado de los esfuerzos conjuntos entre el sector público y privado para enfrentar las amenazas cibernéticas de manera coordinada.

La OEA agradece a ASOBANCARIA por el interés y apoyo en la elaboración de este libro. Gracias a la contribución de expertos de instituciones reconocidas a nivel internacional -como el Centro de Estudios Monetarios Latinoamericanos (CEMLA), la Fiscalía General de la Nación, el Banco Santander, el Banco de Crédito de Perú, la Superintendencia Financiera de Colombia, SWIFT-, y académicos de la Universidad de los Andes, se pudo preparar este libro. En nombre de la Secretaría General de la OEA, quisiera expresar nuestro más sincero agradecimiento por su contribución a esta publicación que, seguramente, será un importante paso en el desarrollo de una cultura de seguridad digital en Colombia y toda nuestra región.

¡Qué disfruten la lectura!

PRÓLOGO
ASOBANCARIA

SANTIAGO CASTRO

Presidente

Asociación Bancaria y de Entidades Financieras de Colombia

Desafíos del riesgo cibernético en el sector financiero para Colombia y América Latina, es el primer libro publicado entre la Asociación Bancaria y Entidades Financieras de Colombia - ASOBANCARIA y la Secretaría General de la Organización de los Estados Americanos (OEA). Se trata de un documento que reúne un conjunto de investigaciones y publicaciones especializadas sobre el estado del arte de la ciberseguridad y su relación con el sistema financiero global, latinoamericano y, en particular, el colombiano.

La Asobancaria se ha propuesto aunar esfuerzos, compartir y difundir conocimientos para poner en marcha una articulación valiosa entre expertos de distintas disciplinas, con el fin de promover reflexiones y acciones en materia de ciberseguridad. En desarrollo de dicho objetivo, el Programa de Ciberseguridad adscrito a la Secretaría del Comité Interamericano contra el Terrorismo (CICTE), entidad que fomenta el diálogo y la cooperación entre los Estados miembros de la OEA para contrarrestar el terrorismo, contribuyó en la definición temática y metodológica de los capítulos.

En el libro se reseñan algunas de las recientes innovaciones y avances tecnológicos en los sistemas productivos y cómo estos pueden afectar la gestión del riesgo cibernético en el sistema financiero en América Latina. Así mismo, se describen algunas tendencias de fraude cibernético y mejores prácticas para prevenir, detectar y responder a incidentes de seguridad. Conocer esto es clave para determinar el rol de los gobiernos y formuladores de política pública para mitigar los riesgos asociados a ciberseguridad.

Actualmente, estamos observando los efectos profundos y sistémicos de la industria 4.0, que se derivan del gran crecimiento de las tecnologías digitales. Es por esto que uno de los grandes desafíos de nuestra sociedad es proteger nuestra información para que solo sea usada por los propietarios o personas autorizadas.

El sector financiero, y en particular la banca, ha sido uno de los sectores con mayores índices de digitalización. Cada día un mayor número de clientes del sector financiero son usuarios de la banca electrónica, realizan transacciones por internet o pagos a través de dispositivos móviles. Esta adaptación de los modelos de negocio y la explotación de canales digitales pretende aprovechar las ventajas de las tecnologías, que tiene como contrapartida la aparición de nuevos riesgos que se deben prevenir con el

fin de mitigar los posibles ataques y situaciones de fraude a los que está expuesto actualmente el sector y, por supuesto, sus usuarios.

Por ello no sorprende que el estudio de la ciberseguridad, entendida como el área de la informática que trabaja en la seguridad de las aplicaciones, servicios o dispositivos para garantizar su confiabilidad o detectar fisuras y solventarlas, se haya convertido en una de las prioridades en las políticas de gestión de riesgo de los gobiernos, creadores de política pública, gremios y sector privado.

El ciberespacio es un sistema complejo a nivel físico, de red y cognitivo. Tradicionalmente, estos sistemas están altamente interconectados y estrechamente acoplados, por lo que las interrupciones pueden conectarse en cascada fácilmente. Este tipo de riesgos son la razón por la cual el ciberespacio es capaz de tener eventos muy impredecibles y de consecuencias altas. Aun no existen modelos que permitan entender y gestionar de forma organizada la complejidad de este riesgo sistémico.

Si bien ningún ataque hasta la fecha ha generado inestabilidad financiera, el impacto potencial de un ataque cibernético programado para desestabilizar las funciones y vulnerabilidades de los canales tradicionales del sistema financiero no se ha examinado lo suficiente. Es claro que la ciberseguridad ya no puede considerarse un tema técnico que se delegue en el departamento de sistemas, sino que debe abordarse como un tema estratégico que alcanza a toda la organización.

En el mundo, gran parte de las comunicaciones y procesos son digitales, con lo cual la ciberseguridad no es una alternativa sino un requisito. Los riesgos cibernéticos que afectan al sector gobierno, al sector privado y a las personas tienen unos impactos y una problemática distintos. No obstante, cada uno debe aplicar medidas de seguridad, adecuándolas a su naturaleza y su propio contexto.

De acuerdo con lo anterior, es prácticamente un hecho que los ataques cibernéticos, el cibercrimen y los incidentes de seguridad no van a disminuir; por el contrario, aumentarán de forma exponencial en los próximos años. Según el Foro Económico Mundial[3], los ataques en contra de empresas casi se han duplicado en cinco años y los incidentes que antes se consideraban algo fuera de lo común se están volviendo más y más recurrentes. Además, el impacto financiero de la ciberdelincuencia va en aumento. Según Inga Beale, ex CEO de Lloyds[4], el costo económico de los ciberataques a nivel mundial será de 6 billones de dólares en 2021.

No siendo ajeno a esta realidad, desde Asobancaria hemos venido desarrollando e implementando una serie de estrategias gremiales. En Colombia, el Comité de Ciberseguridad y Prevención del Fraude actúa como instancia de estudio y consulta del sector financiero en temas de prevención y mitigación del riesgo de fraude y de ciberseguridad, promoviendo las mejores prácticas de seguridad entre las entidades financieras asociadas.

Además, a través del Centro de respuesta de incidentes de ciberseguridad – CSIRT, Asobancaria lidera los esfuerzos de colaboración en el sector financiero para compartir los incidentes de ataques cibernéticos. Sabemos que a través de la colaboración podemos enfrentar este nuevo reto del sector financiero. En un futuro, esta colaboración deberá ser regional, dadas las características y riesgos similares que comparte la banca en Latinoamérica.

El CSIRT financiero conectará a todo el sistema financiero para resolver de manera conjunta los desafíos de ciberseguridad. Es importante tener en cuenta que cuanto más rápido se comparta una amenaza o vulnerabilidad, más posibilidades tienen otras entidades de poner en marcha las defensas para mitigarla. Así mismo, cuantos más datos confiables tengamos, mejores serán las decisiones.

Para avanzar en este proceso de sensibilización entre entidades del sector financiero, el 26 de abril de 2019 realizamos, junto con la Superintendencia Financiera de Colombia, el primer evento de generación de conocimiento dirigido a los presidentes y altas direcciones de las entidades bancarias en materia de ciberseguridad. En este espacio se hizo énfasis en conocer los riesgos cibernéticos emergentes y la importancia de gestionarlos adecuadamente para minimizar los posibles impactos y pérdidas para el sector y sus clientes.

De igual manera, en 2018 realizamos el primer taller de diseño y análisis de escenarios de ciberseguridad del sector financiero colombiano. Así mismo, llevamos a cabo un ejercicio de simulación de amenazas cibernéticas de la industria bancaria colombiana. Ejercicios con los cuales aumentaron los conocimientos de los riesgos y problemas de seguridad asociados con la ejecución de sistemas computarizados, lo que ayudará a promover la confianza en los servicios digitales.

Por su parte, los miembros del Comité de Ciberseguridad y Prevención del Fraude de Asobancaria definieron como prioridad trabajar en la colaboración e intercambio de información entre todo el ecosistema bancario. Esto con el fin de desarrollar estrategias más eficientes que detecten, prevengan, mitiguen y reaccionen ante alertas, eventos e incidentes de ciberseguridad y/o fraude que puedan afectar a las entidades del sector financiero.

En línea con lo anterior, y considerando la importancia de generar nuevas capacidades y conocimiento en los miembros del Comité, entre el 17 y 22 de marzo de 2019 Asobancaria realizó la primera misión de ciberseguridad del sector bancario colombiano a Estados Unidos. Esta misión tuvo como objetivo no solo conocer experiencias y mejores prácticas del sector bancario norteamericano, sino crear un espacio de confianza y comunicación entre los mismos bancos colombianos y de estos con entidades públicas y privadas estadounidenses.

Durante la misión, vicepresidentes, gerentes y directores que tienen a cargo el tema de ciberseguridad en las entidades bancarias tuvieron la oportunidad de conversar y debatir ideas con entidades como la Organización de los Estados Americanos – OEA, SWIFT, FS-ISAC, U.S. Secret Service, Department of Homeland Security, Foro Económico Mundial y Amazon.

Finalmente, en línea con el trabajo que hemos venido realizando, con la publicación de este libro pretendemos que el lector conozca los conceptos clave sobre ciberseguridad y pueda analizar e identificar una serie de brechas y desafíos que persisten en algunas de estas áreas. Adicionalmente, se presentarán algunas sugerencias sobre sus causas subyacentes, las cuales esperamos que contribuyan a enriquecer el conocimiento y las discusiones entre profesionales y formuladores de política pública.

REGIONAL E INTERNACIONAL

El Estado de la Ciberseguridad en el Sector Financiero en Lationamérica y el Caribe

Belisario Contreras, Jorge Bejarano, Orlando Garcés

La Secretaría General de la Organización de los Estados Americanos (OEA), a través del Programa de Ciberseguridad adscrito a la Secretaría del Comité Interamericano contra el Terrorismo (CICTE), promueve y coordina la cooperación entre los Estados Miembros de la OEA y, entre ellos, el Sistema Interamericano y otros organismos en el sistema internacional, con el fin de acceder, prevenir, confrontar, y responder de manera efectiva a las amenazas a la seguridad, a efectos de ser el principal punto de referencia en el hemisferio para desarrollar la cooperación y la creación de capacidad en sus Estados Miembros.

Es así como, durante casi dos décadas, la Secretaría General de la OEA ha venido aportando de manera significativa al fortalecimiento de las capacidades de ciberseguridad en Latinoamérica y el Caribe. Desde entonces, se han aprobado diferentes resoluciones y mandatos, los cuales han venido guiando el trabajo en la materia, para la creación de una cultura de seguridad cibernética con un enfoque multidimensional y multidisciplinario en la región.

Con este tipo de esfuerzos se fortalece la agenda sobre ciberseguridad digital para las Américas, que se estructura en torno a tres (3) pilares: (i) el desarrollo normativo, especialmente el apoyo en la formulación, discusión y socialización de políticas nacionales de ciberseguridad; (ii) el fortalecimiento de capacidades para disfrutar de las oportunidades que aportan el desarrollo de las Tecnologías de la Información y las Comunicaciones (TIC), pero también para hacer frente a los riesgos asociados; y (iii) la ejecución de actividades de investigación y gestión del conocimiento en ciberseguridad.

Específicamente en lo relacionados con las actividades de investigación y gestión del conocimiento en ciberseguridad, se pretende ofrecer a los Estados Miembros documentos técnicos e informes basados en investigaciones para guiar a los responsables de políticas, equipos de respuesta a incidentes (CSIRT), operadores de infraestructura, organizaciones públicas y privadas y la sociedad civil, en aquellos aspectos asociados a los desarrollos actuales e identificando los problemas y desafíos clave de seguridad cibernética en la región. Este tipo de estudios y reportes son esenciales para priorizar la realización de actividades que contrarresten los problemas y desafíos identificados siendo base fundamental para orientaciones de políticas, estrategias, planes y programas y en general, para el desarrollo de capacidades en esta materia.

Este desarrollo de estudios y reportes es complementario a todo el apoyo que se viene dando a los países de la región, en cuanto al desarrollo de sus capacidades técnicas, a la elaboración de diferentes marcos y políticas nacionales de seguridad cibernética. También se han ofrecido diferentes misiones y asesoramientos técnicos, con la clara convicción de elevar la seguridad digital de la región, para procurar maximizar el beneficio del acceso y uso de las TIC en la región y a su vez facilitar el ejercicio de los derechos de todos sus ciudadanos.

Uno de los retos, al abordar los aspectos de seguridad cibernética, es entender su dinámica y de este modo priorizar acciones para fortalecerla. A lo largo del tiempo y con la evolución de las TIC, el sector financiero,

y en particular el sector bancario, ha sido uno de las industrias con mayores índices de digitalización. Cada día un mayor número de clientes del sector financiero son usuarios de la banca electrónica, realizan transacciones por internet o pagos a través de dispositivos móviles y las tendencias mundiales actuales son resultado de los procesos de adaptación que se vienen requiriendo para que los mercados financieros estén en sintonía con los nuevos patrones de la economía digital[5].

Esta evolución de los modelos de negocio y el aprovechamiento de canales digitales pretenden servirse de las ventajas de las tecnologías, las cuales ofrecen ventajas invaluables, pero a la vez traen consigo la aparición de nuevos riesgos que están llamados a ser prevenidos y enfrentados con el fin mitigar los posibles ataques y situaciones de fraude a los que están expuestos actualmente el sector financiero y, por supuesto sus usuarios.

Igualmente, es evidente que la disrupción digital en los mercados financieros ha promovido la inclusión financiera, que actualmente configura un componente fundamental dentro del propósito de reducción de índices de pobreza y promoción de desarrollo en el hemisferio, pues implica el acceso a servicios y productos financieros beneficiosos, eficientes, y alcanzables que atiendan de manera efectiva las necesidades de las personas. Dichos servicios deben ser prestados de manera responsable y sostenible[6]. La inclusión financiera se ha convertido en una prioridad para los gobiernos, los órganos encargados de las reglamentaciones y los organismos de desarrollo a nivel mundial. De hecho, se ha determinado que es un factor que propicia siete de los diecisiete Objetivos de Desarrollo Sostenible establecidos por la Organización de las Naciones Unidas (ONU)[7].

De esta manera, los sistemas financieros revisten de alta importancia; particularmente su acceso y digitalización, pues estos simplifican el diario vivir de los ciudadanos y favorecen la planificación de los agentes económicos. Prueba de ello es que durante los últimos años se ha presenciado una clara expansión de la prestación y de la popularidad de los servicios bancarios móviles y online, pues prácticamente la totalidad de los productos o servicios ofrecidos por las instituciones financieras dependen de la tecnología. Esta colaboración se traduce en una serie de ofertas de productos, proporciona una experiencia de cliente positiva y garantiza que los servicios y las empresas operen de manera eficiente. Incluso los países que han logrado más avances con miras a la inclusión financiera son los que han creado un entorno normativo y reglamentario propicio, y han fomentado la competencia, permitiéndoles a las instituciones bancarias y no bancarias innovar y ampliar el acceso a servicios financieros[8].

Sin embargo, la creación de este espacio innovador y competitivo trae consigo riesgos que deben ser prevenidos y mitigados de manera oportuna, lo cual pone de plano la necesidad de acompañar esta realidad de reglamentaciones y medidas de protección del usuario y del sector bancario en general. Estas medidas deben ser apropiadas para garantizar la prestación responsable de servicios financieros. Es así como la digitalización de esta industria debe tener en cuenta la gestión de ciberdelitos, dado que establecer ambientes digitales implica también analizar riesgos cibernéticos que se deben evitar y manejar adecuadamente.

Así las cosas, la disrupción digital en los mercados financieros no debe ser un tema de preocupación solamente de los actores privados en la búsqueda de alcanzar sus objetivos empresariales, sino que es evidente además, que los retos que se plantean para los Estados reguladores resultan ser de absoluta importancia. Es igualmente vital la forma en que estos son abordados, debido a que se constituyen en una parte fundamental para la construcción de un ecosistema armonioso y acorde con las tendencias que influyen sobre los mismos[9].

En ese mismo sentido, los países que han permitido y favorecido la inclusión financiera han evidenciado obstáculos relacionados con la seguridad digital en el sector bancario y en particular este aspecto se ha convertido en un elemento indispensable a tener en cuenta en relación con la innovación financiera. Con la digitalización de los servicios bancarios, el sector debe procurar ir un paso por delante de la ciberdelincuencia, dada la creciente cantidad de datos de clientes y activos financieros custodiados por los bancos. Incluso según un estudio de WebSense[10], la frecuencia con que las empresas de servicios financieros aseguran sufrir incidentes de seguridad es un 300% superior a la de las empresas de otros sectores.

Lo anterior hace que los temas de ciberseguridad sean muy importantes en el sector financiero, toda vez que, si los clientes y empresas no ven el entorno digital como un espacio confiable y seguro para la realización de sus interacciones, la desconfianza afectaría el uso de los canales digitales y por lo tanto todas las inversiones realizadas en procesos de digitalización de la experiencia del cliente no generaría el impacto positivo esperado. Aunque las organizaciones evidencian su preocupación por el tema y llevan cierto tiempo invirtiendo en seguridad informática, los reiterados y considerables ataques informáticos hacen inevitable que las acciones e inversión en seguridad crezcan.

De hecho, se espera que el gasto en seguridad informática a nivel mundial crezca en cerca de 25% en el año 2020[11], todo ello en un contexto en el que los delitos informáticos siguen en ascenso y así blindar de manera efectiva el mercado financiero digital[12]. En efecto, un estudio realizado por *Business Insider Intelligence* estima que en dicho año se habrán gastado nada menos que $665.000 millones de dólares en proyectos de seguridad electrónica para proteger computadores, dispositivos móviles y dispositivos conectados a internet. El mercado de la seguridad electrónica podría multiplicar por cinco la inversión total en tecnología y se prevé que el costo de estos delitos siga aumentando, tras crecer un 62,5% desde 2013[13].

Es tal la importancia del sistema financiero en los países, que, en el marco de la definición de infraestructuras críticas cibernéticas[14], los países que han abordado la catalogación de este tipo de infraestructuras incluyen al sector financiero como una de ellas, en consideración a la importancia que representa frente a servicios esenciales prestados a nuestros ciudadanos y también para garantizar la estabilidad económica de nuestros países. El sector financiero, por su naturaleza y función, también es una de las infraestructuras críticas regionales que debe ser protegida por sistemas de seguridad efectivos que garanticen su continuidad por parte de los Estados.

Es por todo lo anterior, que la Secretaría General de la OEA ha determinado apoyar a la región Latinoamérica y el Caribe, en la realización de estudios sobre el impacto de la ciberseguridad y la forma como esta afecta el sistema financiero en la región. El primero de estos estudios titulado: “Ciberseguridad: Estado del Sector Bancario en América Latina y el Caribe”, es un aporte de la Secretaría General de la OEA, que tuvo como propósito brindar información fidedigna sobre el Estado del sector bancario en la región y representa el empeño de la OEA en su tarea de fortalecer las capacidades y nivel de conciencia sobre las crecientes amenazas a la seguridad digital que aborda nuestra región.

En este estudio se analizaron datos de 191 entidades bancarias en 19 países de la región (17% grandes, 48% medianas y 35% pequeñas). Se estima que la muestra de entidades bancarias a partir de las cuales se presentan los resultados de dicho estudio alcanzó unos activos bancarios de USD 1 billón y unas utilidades netas de USD 10,5 mil millones a 31 de diciembre de 2017.

Con relación a la preparación y gobernanza, el estudio concluye que la ciberseguridad se considera como una preocupación de alto riesgo para las instancias de decisión (juntas/consejos directivos)

en las entidades bancarias de la región. No obstante, se encuentra que en la mayoría de este tipo de organizaciones convencer a la alta dirección de la organización es medianamente complejo. Este sector se esfuerza por encontrar el talento adecuado e incorporar expertos cibernéticos en sus organizaciones dados los complejos desafíos actuales.

- En promedio, en el 74% de las entidades se tiene una única área responsable por la seguridad digital.

- En promedio, en el 72% de las entidades la junta directiva recibe reportes periódicos acerca de indicadores y gestión de riesgos.

- En promedio, en el 41% de las entidades en la región existen dos (2) niveles jerárquicos entre el CEO y el máximo responsable de la seguridad digital.

- En promedio, más del 60% de las entidades demuestra apoyo a la gestión del riesgo de seguridad digital, exigiendo la adopción de buenas prácticas de seguridad y fomentando la capacitación y sensibilización en seguridad digital.

- Los estándares, mejores prácticas y marcos metodológicos más implementados son las normas ISO 27001 y COBIT.

- En promedio, el número de miembros del equipo destinado a la seguridad digital es de diecisiete (17), para un banco típico de la región y el 82% considera adecuado que el equipo crezca.

Con relación a la detección y análisis de eventos de seguridad digital, el volumen de eventos totales de seguridad digital continúa multiplicándose y la detección de eventos se convierte en tarea de frecuencia diaria en las entidades bancarias de la región. El uso de soluciones de seguridad basadas en tecnologías digitales emergentes ha sido un factor clave; no obstante, es necesario que dichas organizaciones sigan enfocándose en adaptar nuevas tecnologías y encontrar formas innovadoras de entregar soluciones seguras para proporcionar una mejor experiencia al usuario. Tan solo un tercio de los bancos implementan herramientas, controles o procesos usando *Big Data*.

- En promedio, más del 90% han implementado los cortafuegos y las actualizaciones automatizadas de virus y sistemas.

- Los riesgos de seguridad digital que tienen más atención para este tipo de entidades son: i) robo de base de datos crítica, ii) compromiso de credenciales de usuarios privilegiados, y, iii) pérdida de datos.

- En promedio, el 49% de las entidades bancarias no implementan herramientas, controles o procesos usando tecnologías digitales emergentes. Tan solo el 29% de las entidades han implementado soluciones de *Big Data*.

- En promedio, el 85% de las entidades bancarias de la región han implementado tanto sistemas de detección/prevención de intrusiones (IDS e IPS), como procesos de monitoreo de amenazas y vulnerabilidades

- En promedio, un 26% de las entidades bancarias detectaron estos tipos de eventos mediante sistemas propios.

Con relación a la gestión, respuesta y recuperación ante incidentes de seguridad digital, la mayor adopción de aplicaciones web y móviles en el sector bancario en la región ha hecho que la industria sea propensa a un incremento en los ataques cibernéticos avanzados. La materialización de incidentes digitales se presenta en más de un tercio de las entidades en la región. Es imperativo que los bancos medianos y pequeños actualicen sus estrategias de gestión, respuesta y recuperación ante incidentes y ejecuten periódicamente evaluaciones de madurez junto con las acciones correspondientes derivadas.

- El 92% de las entidades bancarias manifiestan que identificaron algún tipo de evento (ataque exitosos y no exitosos) de seguridad digital.

- Los eventos más comunes fueron el código malicioso o *malware* (80% del total de bancos), ii) la violación de políticas de escritorio limpio (*clear desk*) (63% del total de bancos), y, iii) el *phishing* dirigido para tener acceso a sistemas del banco (57% del total de bancos).

- Un 24% de los bancos detectaron con frecuencia diaria el *malware* y un 22% el *phishing*.

- Los eventos de i) *phishing*, ii) ingeniería social, y, iii) software espía (*malware* o troyanos) fueron los más frecuentes contra sus usuarios de servicios financieros.

- El 37% fueron víctimas de incidentes (ataques exitosos) y la principal motivación fue motivos económicos (79% de las entidades bancarias víctimas).

Con relación al reporte de incidentes de seguridad digital, los mecanismos de reporte son esenciales dentro del proceso de gestión de incidentes, no solo desde la perspectiva de que los usuarios puedan informar su ocurrencia (e incluso obtener una compensación cuando proceda) sino por que constituyen también una fuente para la gestión del conocimiento mismo de los incidentes, si se cuenta con una adecuada articulación con otras instancias del sector privado, así como con agencias del gobierno y las fuerzas del orden. En este sentido, los esfuerzos en cuanto a la disposición de este tipo de mecanismos varían según el tamaño del banco, especialmente frente a los que se ofrecen a clientes de sus servicios.

- En promedio, el 88% de los bancos ofrece un mecanismo para que sus usuarios internos (empleados y contratistas) reporten incidentes (ataques exitosos).

- En promedio, el 61% reporta los ataques sufridos ante una autoridad de aplicación de la ley.

- En promedio, el 64% cuenta con plan de comunicaciones para informar a sus clientes de servicios financieros cuando su información personal se haya visto comprometida.

Con relación a la capacitación y concientización, las entidades bancarias están asegurando que sus empleados estén lo suficientemente informados sobre los procedimientos para identificar amenazas de seguridad digital, responder a cualquier amenaza percibida y mantener el cumplimiento regulatorio.

- El mecanismo más efectivo utilizado por los bancos de la región para concientizar es el desarrollo de capacitaciones internas de información.

- En promedio, el 82% de entidades bancarias cuenta con planes de preparación, respuesta y capacitación.

Con relación al impacto de los incidentes de seguridad digital (presupuesto), para reducir la probabilidad de riesgo y pérdidas por la materialización de incidentes digitales, las entidades bancarias de la región

destinan un presupuesto relevante a la seguridad digital. No obstante, es necesario que las organizaciones estimen el retorno de dichas inversiones e impulsen una mayor inversión en tecnologías y soluciones eficientes.

- El presupuesto destinado a la seguridad digital por una entidad bancaria promedio en la región equivale aproximadamente al 2,09% del EBITDA del año anterior. A medida que el banco es más pequeño, la medida relativa al EBITDA frente al presupuesto es mayor: bancos grandes (1,86% del EBITDA), bancos medianos (2,14% del EBITDA) y bancos pequeños (2,16% del EBITDA).

- En el 46% de los bancos, el presupuesto se mantuvo igual, en el 42% aumentó (debido a cumplimiento regulatorio como causa más común) y en el 10% disminuyó (debido a disminución de la utilidad del banco como causa más común).

- Aumentos en presupuesto difieren si es casa matriz vs. sucursal, subordinada o agencia.

- La distribución del presupuesto es: 43% en plataformas y medios tecnológicos, un 22% en recursos humanos, un 22% en servicios tercerizados y un 13% en generación de capacidades.

Con relación al impacto (costo) de los incidentes de seguridad digital, aunque el costo estimado promedio anual por banco en la región es inferior al presupuesto estimado promedio anual por banco en asuntos de seguridad digital, el sector bancario en la región incurre en unos costos significativos por respuesta y por recuperación ante incidentes de seguridad digital.

- El costo total de respuesta y de recuperación ante incidentes de seguridad digital para una entidad bancaria promedio en la región supone aproximadamente el 1,52% del EBITDA del año anterior.

- A medida que el banco es más pequeño la medida relativa al EBITDA frente al costo es menor: bancos grandes (1,86% del EBITDA que equivale a USD 5 millones aprox. al año), bancos medianos (1,38% del EBITDA que equivale a USD 600.000 aprox. al año) y bancos pequeños (1,36% del EBITDA que equivale a USD 160.000 aprox. al año).

- El costo total aumenta a medida que el tamaño del banco aumenta, independientemente si es casa matriz vs. sucursal.

- Con los valores obtenidos del estudio se estima que el costo total anual de respuesta y de recuperación ante incidentes de seguridad digital de las entidades bancarias de la región América Latina para 2017 fue de USD 809 millones aproximadamente.

El estudio “Ciberseguridad: Estado del Sector Bancario en América Latina y el Caribe”, es una muestra más del liderazgo de las instituciones de la región y la confianza que tienen en la OEA, como lo demuestra la importante participación de bancos de la región, así como la ratificación del compromiso de la Secretaría General de la OEA en seguir acompañando los esfuerzos en materia de seguridad digital en las Américas.

Con base en resultados como los obtenidos con este estudio, se ha logrado avanzar también en reportes nacionales de los Estados en lo referente a cómo se encuentra la ciberseguridad, no solamente en el sector bancario, sino del sistema financiero en su totalidad; tal como ocurrió en el caso de México. Es así como a través del estudio “Estado de la Ciberseguridad en el Sistema Financiero Mexicano”, se abordaron

240 entidades/instituciones del sistema financiero mexicano, de las cuales 98 son sociedades de ahorro y crédito popular, 59 pertenecen al sector de intermediarios financieros no bancarios, 33 integrantes de la banca comercial y de servicios múltiples, 17 instituciones de tecnología financiera, 15 sociedades financieras populares, nueve bancos de desarrollo y nueve integrantes del sector bursátil.

En este estudio, se estableció una base de datos con registros de 240 entidades con cobertura en los 32 estados de México, en su mayoría ubicados en la Ciudad de México (30%). La muestra representa el 63% de las entidades/instituciones financieras del país. Estas entidades forman parte del sector bancario, el sector de ahorro y crédito popular, el sector de intermediarios financieros no bancarios, el sector de intermediarios del mercado de valores y el sector de fintech. Se estima que la muestra de entidades/instituciones alcanzó activos cercanos a 700.000 millones de dólares estadounidenses al 31 de diciembre de 2018, lo que representa aproximadamente el 87% de los activos totales de estos sectores, y ganancias netas superiores a 7.000 millones de dólares estadounidenses al 31 de diciembre de 2018. También dicha muestra presta servicios a más de 46 millones de clientes (socios, asociados o usuarios de servicios financieros) en el país. Se destaca que el 78% de dichos clientes son usuarios de servicios bancarios.

Con relación a la preparación y gobernanza, la mayoría de las instituciones/entidades financieras entrevistadas (70%) en México mencionaron que hay una sola área responsable de la seguridad de la información (incluida la ciberseguridad) en su organización. Vale la pena señalar que a medida que la entidad crece, las áreas responsables de la seguridad digital aumentan. El número de niveles jerárquicos entre el CEO y el jefe de seguridad digital en la entidad/institución financiera depende del tamaño de la organización en el país. Por ejemplo, en el 60% de las entidades pequeñas, la persona máxima responsable reporta directamente al CEO, es decir, es un (1) nivel único, mientras que en ninguna entidad grande ocurriría tal situación. Con respecto a las personas que comprenden la totalidad de los equipos que manejan los procesos asociados con la seguridad de la información (incluida la ciberseguridad) y los fraudes que ocurren a través de los medios digitales, en promedio para el sistema financiero mexicano, el 87% de las entidades mencionaron que tienen equipos de entre 1 y 5 personas para manejar la seguridad digital. Esta situación difiere entre sectores, mientras que casi todas las entidades en el sector de ahorro y crédito tienen equipos de hasta 5 miembros, solo la mitad de las entidades en el sector bancario comprenden entre 1 y 5 miembros del personal.

Con relación a la detección y análisis de eventos de seguridad digital, los eventos de seguridad digital más comúnmente identificados por las entidades/instituciones financieras mexicanas durante 2018 fueron i) código malicioso o *malware* (56%), ii) *Phishing, Vishing o Smishing* (47%) y iii) violación de políticas claras de escritorio (31%). Al analizar los resultados con respecto a la frecuencia aproximada de ocurrencia de eventos identificados por las entidades/instituciones financieras en México durante 2018, se puede ver una dinámica particular por tipo de evento que también depende del tamaño de la organización. Por ejemplo, el 19% de las entidades identificaron la ocurrencia de eventos de *malware* a diario, ii) el 20% del total los identificó semanalmente, iii) el 19% del total mensual y iv) el 43% del total trimestralmente. Además, el uso de tecnologías digitales emergentes aplicadas a herramientas, controles o procesos de seguridad digital en entidades/instituciones financieras en México todavía está rezagado. Solo el 22% de las entidades/instituciones financieras implementan análisis de datos en herramientas, controles o procesos, el 13% implementa *Machine Learning* y el 9% implementa Inteligencia artificial.

Con relación a la gestión, respuesta y recuperación ante incidentes de seguridad digital, el 43% de las grandes entidades/instituciones financieras de México fueron víctimas de ataques exitosos, mientras que entre entidades de tamaño el porcentaje es del 15% y entre las pequeñas, del 6%. Se destaca el hecho de que, en el sector bancario de México, el promedio es más alto en comparación con otros sectores del sistema financiero mexicano, informando la materialización de incidentes (ataques exitosos) en 50%

en entidades grandes, 22% en entidades medianas y 11% en entidades pequeñas, sin embargo, es más bajo que los resultados en el sector bancario en la región donde los bancos grandes reportan el 65%, los bancos medianos el 43% y las compañías pequeñas el 19% de las víctimas.

Con relación al reporte de incidentes de seguridad digital, en términos generales, se puede ver que más de la mitad de las entidades/instituciones financieras en México -grandes (86%), medianas (57%) y pequeñas (53%)- ofrecen un mecanismo para sus empleados (empleados y contratistas) para reportar incidentes (ataques exitosos) de la seguridad digital sufrida, y en sectores como el sector bancario, se alcanza el 93%, superando incluso el promedio de la región de América Latina y el Caribe (68% de los bancos de la región). Se aprecia la existencia de mecanismos de reporte para sus clientes (socios, asociados o usuarios) de servicios financieros para informar incidentes a la entidad, la existencia de un plan de comunicaciones que permite a los clientes ser informados cuando su información personal ha sido comprometida y sobre el informe de incidentes (ataques exitosos) ante una autoridad reguladora en México.

Con relación al impacto de los incidentes de seguridad digital, en comparación con el año fiscal inmediatamente anterior, el 57% de las entidades en el país dijo que el presupuesto de seguridad de la información se mantuvo sin cambios, el 38% dijo que había aumentado y solo el 5% dijo que había disminuido. Sin embargo, más del 60% de las entidades en el sector bancario, en el sector de intermediarios del mercado de valores y en el sector de fintech han aumentado, mientras que menos del 30% en el sector de ahorro y crédito y los intermediarios financieros no bancarios lo han hecho. Este presupuesto asignado al año por una entidad/institución financiera promedio del sistema financiero mexicano para la seguridad de la información (incluida la ciberseguridad) se distribuyó de la siguiente manera: 47% para plataformas tecnológicas, 20% para personal, 20% para servicios subcontratados y solo 13% para programas de creación de capacidad. Finalmente, se estima que el costo total de respuesta y recuperación ante incidentes de seguridad digital para una entidad promedio grande en México es de aproximadamente USD 2,3 millones por año, para una entidad de tamaño medio promedio es de aproximadamente USD 634.000 por año y para una entidad promedio pequeña es equivalente a aproximadamente USD 317.000 por año.

Es importante señalar que ambos estudios contemplan un capítulo con un importante conjunto de recomendaciones, entre las que se destacan aspectos como:

- La necesidad de contar con una instancia u órgano de gobierno corporativo para liderar los temas de ciberseguridad, con respaldo y esquema de reporte a las máximas instancias de decisión de las instituciones y que cuente con recursos adecuados para gestionar los riesgos de seguridad digital.

- La relevancia de hacer revisiones revisión habitual de mejores prácticas en marcos de gobierno, seguridad y/o estándares internacionales, así como del marco regulatorio local e internacional aplicable a los diversos sectores y entidades/instituciones financieras, haciendo un proceso de mapeo y priorización para su adecuada aplicación.

- La importancia de garantizar que la priorización de acciones, procesos y programas de seguridad digital para proteger los sistemas de información críticos de la entidad/institución financiera, corresponden a un plan derivado de las necesidades de adopción y aplicación de marcos regulatorios (local e internacional), mejores prácticas y/o estándares internacionales. Resulta relevante que este plan tenga, como uno de sus focos objetivo, el elevar la resiliencia cibernética.

- La necesidad de priorizar el desarrollo de capacidades usando tecnologías digitales emergentes, tales como *Big Data*, Inteligencia Artificial y sus relacionadas (tales como computación cognitiva y *Machine Learning*), que tienen un importante potencial en la optimización de recursos destinados a la detección y prevención de riesgos de seguridad digital.

- La necesidad de apoyar las investigaciones y seguir los protocolos exigidos por las autoridades de procuración de justicia y las mejores prácticas aplicables a la cadena de custodia de la evidencia digital (por ejemplo, que faciliten la cooperación nacional e internacional), que resulten relevantes para los procesos investigativos.

- La relevancia de participar activamente en alianzas en las que se logre compartir las conclusiones y lecciones aprendidas sobre la gestión de eventos (ataques exitosos y ataques no exitosos), que faciliten la identificación y prevención de delitos, así como el desarrollo de soluciones holísticas para gestionar el riesgo cibernético.

- La importancia de disponer planes de capacitación con públicos objetivos y específicos (empleados internos, insourcing, proveedores, clientes, nivel ejecutivo, etc.) que se orienten a elevar la cultura de seguridad digital, el desarrollo de capacidades y la sensibilización (según sea el caso), garantizando su ejecución periódica y estableciendo evaluaciones a efecto de determinar su impacto.

- La relevancia de comunicar estratégicamente a la alta dirección y órganos de gobierno que los recursos destinados a seguridad digital no son un costo, sino realmente una inversión y que la protección contra incidentes digitales debe ser parte integral de la estrategia de negocio, dado el alto impacto y repercusión que se pueden derivar de su ocurrencia. Estimar una tasa interna de retorno de las inversiones efectuadas en seguridad digital.

La experiencia con estos dos (2) estudios, si bien muestra coincidencias en algunos de los hallazgos y recomendaciones, también permite valorar la importancia de hacer la evaluación del estado de ciberseguridad, en el contexto y condiciones particulares de un país. Además, el hecho de realizar el primer estudio teniendo como ámbito de estudio el sector Bancario de América Latina y el Caribe y luego aplicarlo en un país, pero ampliando su aplicación a todo un sistema financiero, permite que los hallazgos puedan verse con una mejor "resolución", es decir, con un mejor detalle, lo que permite identificar diferencias entre los diferentes sectores que lo conforman y orientar mejor las recomendaciones y acciones que deberían adelantarse según corresponda, así como los actores particulares que podrían impulsarlas.

Ahora bien, Colombia no se queda atrás en términos de valorar la importancia de contar con un diagnóstico de cómo se encuentran los aspectos de seguridad digital en su sistema financiero, toda vez que la OEA a través de un convenio con la Asociación Bancaria y de Entidades Financieras de Colombia (ASOBANCARIA), abordó la realización de este libro, en el cual se tratan los temas más relevantes para las entidades financieras con respecto a las mejores prácticas y tendencias de la ciberseguridad. Además, con base en las experiencias tanto regional como nacional que tiene la organización en estos estudios, incluye el análisis sobre las tendencias de las amenazas, capacidades de gestión y medidas de seguridad adoptadas, así como el impacto que han tenido los incidentes digitales en las instituciones y usuarios del sistema, entre otros aspectos. Estos resultados permitirán conocer mejor cómo está el país en esta materia y en qué aspectos enfocar las acciones que mejoren y eleven la confianza en el uso del entorno digital, por parte de las organizaciones y usuarios del sistema financiero en Colombia.

Para terminar, vale la pena destacar que los países de Latinoamérica y el Caribe han hecho un esfuerzo significativo para transformarse digitalmente. Esto implica un grado de avance importante pero aún queda mucho por hacer. El mercado y el consumidor continúan evolucionando, por lo cual se reitera el agradecimiento a los gobiernos de la región, quienes, por más una vez, han confiado en el trabajo de la OEA en la ejecución eficiente de acciones para materializar un entorno digital confiable y seguro, que resulte propicio para sus iniciativas de transformación digital, y con ellas, el desarrollo económico y social de los pueblos. Para la organización es totalmente claro que más internet equivale a menos pobreza y mayor productividad en los territorios, lo cual en último término se traduce en oportunidades de generación de más y mayores derechos para más personas.

Cooperación internacional y su papel en la gestión del riesgo cibernético

Raúl Morales Reséndiz

Introducción

La crisis financiera global planteó distintos cuestionamientos sobre la capacidad de las autoridades financieras para responder al desarrollo y funcionamiento de un sistema financiero complejo, considerablemente más interconectado y dispuesto a asumir riesgos más allá de su papel de intermediadores entre prestamistas y ahorradores.

Como resultado de esta crisis, la comunidad financiera internacional generó una respuesta sin precedentes para ir remediando los distintos aspectos de la regulación y supervisión financiera que presentaron alguna vulnerabilidad, y también para fortalecer los estándares de regulación para el sistema financiero, con un énfasis especial en la conducta y disciplina de mercado y en la transparencia de la información. Al día de hoy resulta difícil anticipar qué riesgos financieros podrían desatar una nueva crisis a nivel internacional, pero han surgido nuevos elementos en el ecosistema que por su naturaleza se han convertido en temas de gran preocupación para la estabilidad financiera, el riesgo cibernético y la llegada de nuevas tecnologías financieras.

Los ataques cibernéticos, como un acontecimiento cada vez más común, han puesto de manifiesto la necesidad de que las autoridades establezcan un cerco de seguridad que sirva a las entidades del sistema financiero de escudo para no ser tan vulnerables ante posibles ataques de los delincuentes cibernéticos.

La naturaleza del riesgo cibernético y la experiencia de la regulación financiera reciente permiten concluir que la coordinación y cooperación internacional son los pilares de una estrategia de seguridad cibernética basada en mejores prácticas domésticas y en una mayor cooperación interinstitucional que incluya, además, la participación de agencias gubernamentales relevantes, que van más allá del ámbito financiero. Esfuerzos de esta naturaleza se vienen llevando a cabo de manera reciente, como por ejemplo la estrategia para reducir el riesgo cibernético en los sistemas de pago de alto valor, que es promovida por el Comité de Pagos e Infraestructuras de Mercado, o bien el Marco Europeo de Hacking Ético basado en Inteligencia de Amenazas (TIBER-UE) del Banco Central Europeo (BCE).

El riesgo cibernético como un fenómeno transfronterizo

El sector financiero es por excelencia una actividad económica en la que la innovación y el uso de las tecnologías de información son fundamentales. Visto en una forma simple, una entidad financiera es autorizada a realizar intermediación de ahorros y préstamos, apalancándose en los primeros para poder crear dinero. Para llevar adelante esta tarea, las entidades requieren de un sistema de transmisión de información; es decir, de mecanismos, reglas y vías para transmitir fondos, enviar y recibir pagos, lo cual es una actividad intensiva en el uso de las tecnologías de información.

Con el aprovechamiento de las tecnologías de información y comunicación, en años recientes, el sistema financiero ha podido generar eficiencias muy importantes y con ello responder mejor a las necesidades de los usuarios de servicios financieros, a nivel individual, corporativo y gubernamental. A cambio de ello, hoy en día esa dependencia de la información y de las tecnologías relacionadas en el desarrollo, ha elevado el riesgo de su gestión, lo cual se ha traducido en mayores índices y probabilidad de ser vulnerable a ataques cibernéticos. Esto es más evidente cuando se considera que el papel central del sistema financiero es movilizar recursos económicos, dinero, entre agentes económicos a través de sus redes y sistemas de comunicación. Si a esto se añade el hecho de que la globalización se ha acentuado mucho más en el sector financiero a nivel mundial, con esto se tiene un contexto en el que los criminales cibernéticos encuentran condiciones atractivas para hacer uso continuo y cada vez más sofisticado de sus recursos para poner en riesgo el dinero y la información de los agentes económicos.

Un ejemplo claro sobre las oportunidades que ha abierto la globalización financiera al riesgo cibernético es a través de SWIFT, que es una red de mensajería global única y que permite la interconectividad entre entidades financieras, instituciones oficiales y otros usuarios de dicha red para transferir información sobre pagos entre agentes económicos de distintas jurisdicciones. Esta compañía ha logrado consolidarse como un mecanismo único de transmisión de información financiera y, al mismo tiempo, ha concentrado un peso importante de las comunicaciones de los sistemas de pago a nivel mundial, basándose en estándares propietarios y haciendo un uso intensivo de tecnologías de información y comunicación. Con todas estas características, las posibilidades de un ataque cibernético no han sido menores y, de hecho, como ocurrió entre 2016 y 2018, ha habido una serie de intentos y ataques consumados a puntos de acceso (fuera de la red SWIFT) de este participante global del sistema financiero, reflejando que cada vez más el carácter del riesgo cibernético trasciende a dimensiones transfronterizas.

Como ha sido el caso de otros fenómenos en el mundo financiero que adquieren un matiz transfronterizo, las posibilidades y opciones para acompañar con un marco de políticas y estándares se multiplican, especialmente ante la necesidad de evitar que una falta de armonización abra la puerta a opciones adicionales de arbitraje regulatorio. Sin embargo, en el caso del riesgo cibernético la situación es completamente distinta a otros eventos o fenómenos transfronterizos.

La naturaleza evolutiva de los riesgos en el sistema financiero son definitivamente una cuestión de interés público, por ello el riesgo cibernético se encuentra en las prioridades más relevantes en la actualidad para las autoridades financieras. El hecho de que el riesgo cibernético sea tan cambiante no es una cuestión imprevista, dado que el sector financiero es una actividad económica que hace un uso intensivo de las tecnologías de información y comunicación, pero la complejidad de este nuevo fenómeno de naturaleza global y amenazante para la economía mundial es el grado de interconexión e interdependencia que existe en el sistema financiero internacional. Aún economías pequeñas con sistemas financieros en proceso de desarrollo pueden sufrir los estragos de episodios de tensión o cambio en grandes centros financieros internacionales; por ejemplo, la reforma financiera en Estados Unidos de Norteamérica, entre otros motivos, obligó a grandes bancos internacionales —con matriz en ese país— a endurecer sus políticas de servicios de corresponsalía bancaria, y dejó incomunicados sistemas financieros de varias economías pequeñas, como fue el caso de los países que conforman la subregión del Caribe. En el caso del riesgo cibernético, la dinámica del sistema financiero internacional ha mostrado que el potencial de contagio es incalculable y posiblemente de muy alto impacto a nivel doméstico, pero también a nivel transfronterizo. Todo esto exige un seguimiento y una evaluación mucho más coordinada por parte de las distintas autoridades financieras de cada país, y para ello, resulta —en primer lugar— fundamental comprender y reconocer las implicaciones para la estabilidad financiera de un ataque cibernético. Desde luego, esto es una tarea compleja en un contexto de cambio general y de aparición de nuevos patrones y estructuras de mercado en el sector financiero. Puesto de una forma, con un sector tecnofinanciero (fintech) en

crecimiento, la perseverancia de entidades no bancarias operando bajo la sombra y una cadena de valor que constantemente se fragmenta más, entender adecuadamente las funciones y responsabilidades de todas las partes de un ecosistema en cuanto al manejo de la información y los datos que transitan por el sistema financiero no es una cuestión menor e incluso es materia de un tratamiento que va mucho más allá del propio riesgo cibernético y sobre el que ya está trabajando la comunidad financiera internacional. De otra, las autoridades financieras tradicionalmente actuaban bajo un perímetro de regulación y supervisión bien conocido y con un conjunto de herramientas que se fueron consolidando con el paso del tiempo para asegurar que las entidades financieras cumplían y se adecuaban a la normativa vigente, pero hoy en día, y no solo en el caso del riesgo cibernético, la proliferación de nuevos proveedores de servicios financieros y de otros servicios auxiliares ha mostrado que si bien se ha ganado a nivel de competencia y eficiencia, también se ha comprometido en materia de seguridad. En un gran número de incidentes cibernéticos, de un modo u otro, se puede ver cómo terceras partes que están brindando servicios de comunicación y acceso a entidades financieras, infraestructuras de mercado y otras plataformas críticas y relevantes para el sistema financiero, han tenido un papel importante en el surgimiento de este riesgo, sin que las autoridades estén en condiciones de anticipar o reaccionar adecuadamente; en una escala transfronteriza, las implicaciones son aún más complejas debido a que al analizar estos incidentes no necesariamente se puede fincar responsabilidades entre las distintas jurisdicciones involucradas y aun si se pudiera, las probabilidades de que una autoridad financiera tenga la posibilidad de actuar en tiempo, su influencia fuera del ámbito nacional puede estar limitado si no existe comunicación o mecanismos de coordinación con otras autoridades de más países.

El papel de las autoridades financieras

Las autoridades financieras, especialmente luego de la Crisis Financiera Global, han quedado más expuestas al escrutinio de la sociedad como principales responsables de preservar la estabilidad monetaria y promover la estabilidad financiera. Sin embargo, la complejidad que ha primado en el desarrollo del sistema financiero requiere que, en la actualidad, las autoridades financieras tengan un papel más efectivo de coordinación y cooperación internacional, para el diseño de mecanismos eficaces para la atención de nuevas necesidades (riesgos y amenazas) que surgen en el sistema financiero.

Como parte de ello, es fundamental que las autoridades financieras cuenten con políticas de buen gobierno, especialmente en lo referente a sus funciones clave, ya que suele implicar tomar decisiones y coordinarse entre sí, para resolver dificultades que van surgiendo en los distintos mercados y el sistema financiero en su conjunto; esto es de especial relevancia, si se toma en consideración que un objetivo primario de la administración pública es velar por el bienestar social y resolver fallas que los agentes económicos, especialmente del sector privado, no son capaces de resolver. Las prioridades, objetivos y compromisos de las autoridades financieras difieren considerablemente entre países, aunque algunos aspectos son comunes a todos ellos. Esto hace que la coordinación y cooperación internacional no resulte una cuestión trivial.

Recientemente, y especialmente en el ámbito de la estabilidad financiera, se ha avanzado considerablemente en aras de tener un marco de políticas y estándares internacionales enfocados en promover sistemas financieros saludables a nivel global. Por ejemplo, el Comité de Supervisión Bancaria de Basilea (BCBS) del Banco de Pagos Internacionales (BIS) emitió una trascendental reforma del Marco de Basilea y que en la actualidad se le denomina como Basilea III. Otra instancia de intensa revisión y coordinación luego de la CFG es la de los mercados de activos financieros, particularmente aquellos no estandarizados (OTC), que por las vulnerabilidades que presentaron llevaron a que la Organización Internacional de Comisiones de Valores (IOSCO, por sus siglas en inglés) estableciera en coordinación con otros organismos internacionales en un amplio marco general para la regulación de dichos mercados,

contemplando los instrumentos y activos que se negocian en ellos, los intermediarios que operan y se relacionan entre sí, los emisores de valores o activos financieros, las entidades que ofrecen servicios analíticos o de evaluación, como las agencias calificadoras, y la gestión y operación de esquemas de inversión colectiva.

Este marco de políticas y estándares internacionales representan un acuerdo del más alto nivel entre autoridades financieras de todo el mundo que sirven de base para armonizar y coordinar las acciones de regulación y de política financiera para hacer que los sistemas financieros sean confiables y robustos. Puesto así, el hecho de que cada autoridad financiera -a nivel doméstico, regional e internacional- trabaje en aras de una implementación completa, oportuna y consistente de estas mejores prácticas, bajo la coordinación de entes que se encargan de trabajar en el desarrollo de estos estándares resulta crucial para lograr una regulación coherente a nivel internacional.

Respecto de esto último y en relación al riesgo cibernético, la importancia de la coordinación y la cooperación en el ámbito transfronterizo se torna mucho más relevante, dada la naturaleza y complejidad del fenómeno. En este contexto, los ministros de Finanzas y gobernadores de bancos centrales del G20 reconocieron en marzo de 2017 que "el uso malicioso de las tecnologías de la información y la comunicación (TIC) podrían tener consecuencias importantes para los sistemas financieros nacionales e internacionales, poniendo así en riesgo la estabilidad financiera y socavar la confianza de los agentes económicos en el sector financiero".

Y es que inclusive fuera del ámbito transfronterizo, los bancos centrales y las agencias de supervisión financiera tienen más que nunca una labor misional de velar por la estabilidad financiera, por lo que el riesgo cibernético se constituye como un desafío de la mayor prioridad, tanto por la necesidad de establecer un común acuerdo de qué implica este fenómeno, como por definir el terreno regulatorio que abarca y que –muy probablemente– demandará que las autoridades financieras revisen su marco general de gestión de riesgos en un sentido que se precise y establezca de manera explícita la importancia, las formas, los mecanismos y las posibles consecuencias de atender eventos de tipo cibernético. Esto asegurará que las autoridades pertinentes y las entidades financieras, infraestructuras de mercado y otros agentes relevantes estén mejor preparados para identificar, responder y recuperarse de eventos de esta naturaleza. En todos los casos, cada parte del ecosistema requiere orientación para responder a cuestiones fundamentales asociadas con el riesgo cibernético, como por ejemplo, se necesitan herramientas y cuáles son las más adecuadas para enfrentar este nuevo reto operacional y regulatorio; o bien, cómo se debe estructurar la toma de decisiones en torno a este riesgo tan complejo y transversal a las organizaciones, mercados y actividades económicas, para asegurar que existen líneas de responsabilidad y acción apropiadas que en caso de incidentes son fundamentales para actuar con urgencia y tener claridad sobre los procesos de consulta y colaboración interinstitucional; o por otra parte, cómo se deben estimar las posibles consecuencias e implicaciones de un fenómeno que está en constante cambio y evolución para que el marco de gestión de riesgos refleje adecuadamente la gravedad que puede tener este fenómeno para el sistema financiero y las economías; o en un sentido menos favorable, qué mecanismos deben existir para soportar las pérdidas en caso de producirse, la capacidad de recuperación y las acciones posteriores que habrán de tomarse para aprender de eventos cibernéticos.

Todas estas cuestiones también son aplicables en un contexto transfronterizo, aunque con un mayor grado de complejidad. Los propios análisis y medidas de política son más difíciles de llevar a cabo al incluir distintos enfoques regulatorios, capacidad institucional y variedad de parámetros y medidas acerca del riesgo cibernético. Además, como se ha mencionado, se trata de una nueva forma de riesgo que involucra un mayor número de instituciones públicas y privadas involucradas. Con todo, como un evento de riesgo

cibernético puede afectar más allá de las fronteras de una jurisdicción en la que ocurra, especialmente a través de las conexiones de grupos financieros transfronterizos o de sectores económicos estrechamente relacionados, las autoridades financieras tienen un papel central en asegurar que esta dimensión es contemplada dentro de la estrategia, políticas o acciones que se promuevan al respecto. Por ejemplo, se puede considerar que hay distintos niveles de coordinación internacional que se pueden contemplar; en el caso de entidades financieras que tienen presencia regional, infraestructuras de mercado que sirven mercados en distintas jurisdicciones o economías con estrechos vínculos, por ejemplo, Centroamérica. Los aspectos transfronterizos son así relevantes tanto como para preparar las relaciones institucionales, los mandatos e instrumentos en un sentido armonizable que favorezca la cooperación internacional durante eventos o incidentes cibernéticos; el ejemplo más claro de ello, es la urgente necesidad de intercambiar información sensible entre autoridades de supervisión de distintos países en el evento de que una entidad de importancia sistémica sufra un ataque cibernético y pueda contagiar a sistemas financieros donde dicha entidad tiene una presencia, relaciones o funciones de carácter considerable.

Prácticas regulatorias de seguridad cibernética

De acuerdo con el Instituto de Estabilidad Financiera del BIS, son pocas las economías a nivel mundial que cuentan con regulaciones explícitas y marcos o políticas en vigor para el riesgo cibernético. Dentro de este grupo de naciones se encuentran Estados Unidos, el Eurosistema, Hong Kong, México, Reino Unido y República Dominicana, por mencionar algunos. Por otra parte, considerando la naturaleza de este fenómeno, también se debe mencionar que hay un gran número de economías que ya cuentan con una regulación relativa a la tecnología y al riesgo operacional y que han aprovechado este marco para tender medidas que alcancen al riesgo cibernético, en alguna forma. Pero, con todo y esto, hay todavía algunas economías que están trabajando en adoptar algún tipo de medida al respecto, e incluso aquellos que ya han avanzado están enfrentándose a la complejidad de un fenómeno que evoluciona rápidamente y que requiere que las instituciones públicas y privadas se equipen con herramientas y capacidades mínimas para responder al riesgo cibernético en sus distintas etapas; su identificación, seguimiento, tratamiento y recuperación.

Para las autoridades que ya han desarrollado un marco regulatorio específico, se presenta el reto de establecer parámetros y políticas de tolerancia al riesgo, así como identificar escenarios realistas que puedan ser verificables y actualizables con regularidad. Más importante que eso, aun teniendo un marco para la regulación y supervisión del riesgo cibernético, es de la mayor importancia que a las entidades financieras, infraestructuras y otros actores relevantes se les exija supervisar las políticas propias de seguridad cibernética a partir de un conjunto mínimo de expectativas y lineamientos que favorezcan un campo nivelado para que las autoridades verifiquen que la aplicación de tales medidas sea consistente entre entidades y a nivel de todo el sistema. Dichas expectativas tienen que ver con la necesidad de que todas las partes que conforman el ecosistema financiero de una jurisdicción contribuyan individualmente a asegurar su perímetro de actuación y que las autoridades reconozcan los distintos vectores de riesgo; entre las acciones que esto implica se encuentran la identificación de información crítica, ejercicios de vulnerabilidad y resistencia al riesgo cibernético (que se conocen como pruebas de penetración), incluso entre terceras partes que tienen un papel importante en la provisión de servicios de comunicación y funcionalidad en los mercados financieros, así como la inmediata comunicación con las autoridades durante eventos o incidentes cibernéticos, pero también el establecimiento de un buen gobierno y una cultura institucional acerca del riesgo cibernético y el manejo de la información dentro del sistema financiero. Aunado a esto, es indispensable contemplar que las autoridades deben ser todavía más activas que el conjunto de entidades para transformar toda la información que se genera a nivel micro y con esto desarrollar una inteligencia y marco de comunicación y respuesta con actores clave; por ejemplo, conformar grupos de inteligencia que se dediquen a analizar la información y sean capaces de

traducir esto en el diseño de pruebas similares que retroalimenten a las entidades que están ejerciendo la seguridad cibernética y a las autoridades en identificar puntos de atención en eventos o incidentes de este tipo.

Para las autoridades que opten por utilizar su normativa de riesgo tecnológico o riesgo operacional, los elementos de seguridad cibernética deben reforzarse considerablemente ante la necesidad de enviar una señal fuerte al sistema financiero de que esta nueva forma de riesgo es relevante y requiere de un adecuado tratamiento. Por encima de esto, las autoridades también deberán ser más arrojadas a proponer un marco tipo de políticas de seguridad cibernética y con ello establecer los parámetros generales sobre los que los participantes del sistema financiero tendrán que elaborar para desarrollar sus propias estrategias contra el riesgo cibernético. El seguimiento de estas acciones será también una tarea que las autoridades pertinentes tendrán que desarrollar, y para ello será indispensable que se cuente con el personal y las calificaciones apropiadas para validar que las medidas tomadas realmente contribuyen a la contención de este tipo de amenazas; y, particularmente, para poder prescribir revisiones vinculantes y que promuevan una armonización constante en todo tipo de entidades, infraestructuras y actores relevantes dentro del ecosistema financiero.

Para todo esto, resulta útil contar con puntos de partida o mejores prácticas, estándares o normas técnicas, tanto domésticas como de carácter internacional. El Comité de Supervisión Bancaria de Basilea ha señalado que la mayoría de los supervisores a nivel mundial actúan bajo esta lógica, aprovechando desarrollos nacionales o estándares internacionales; respecto de estas últimas, se pueden mencionar el marco de trabajo del National Institute of Standards and Technology (NIST) de Estados Unidos, el ISO 27000 y el marco de trabajo del Comité de Pagos e Infraestructuras de Mercado. En el siguiente capítulo se profundiza en estas prácticas de carácter internacional.

A nivel de experiencias nacionales, se debe primero señalar que los aspectos institucionales, legales e idiosincráticos de cada jurisdicción hacen que sea imposible pensar que este tipo de orientación se pueda convertir en un estándar a nivel internacional, aun cuando el NIST o el marco del Banco Central Europeo sí se puedan considerar estándares nacionales (o regional) con amplia aceptación; no obstante, se puede reconocer que la experiencia doméstica de las distintas economías que han avanzado en materia de riesgo cibernético puede arrojar luz sobre acciones y componentes de una estrategia con resultados favorables, o bien sobre aspectos que se pueden mejorar o adaptar de cierta forma en otras jurisdicciones.

En el caso de México, con motivo de un incidente cibernético de escala considerable en una de las principales infraestructuras financieras de ese país, se revisaron profundamente las prácticas de gestión del riesgo cibernético y se estableció una estrategia de ciberseguridad encabezada por el banco central en coordinación con un consejo de orden nacional que vela por la estabilidad financiera en México. Bajo esta nueva estrategia, el banco central adopta una postura sumamente activa en el manejo del riesgo cibernético yendo más allá de la seguridad de las redes de comunicación financiera, la seguridad del sistema de información y las amenazas de seguridad cibernética, sino que ahora tiene un papel preponderante en el seguimiento y control de la seguridad de la información entre las principales infraestructuras y entidades del sistema financiero, incluyendo conceptos tales como: a) gobernanza, b) políticas, c) procedimientos para incidentes (prevención, detección, respuesta y recuperación), d) concientización y e) colaboración. Con todo este cambio, el banco central busca una estrategia centrada en el flujo de información y los canales que atraviesa esta en el sistema financiero, incluyendo participantes directos y terceras partes también. Para ello, se establece en la regulación que existan mecanismos de control de seguridad de la información, por ejemplo acerca de quién y cómo decide sobre los estándares que se van a emplear, por ejemplo, que se identifique y responsabilice a un equipo o a personas con

la autoridad para conducir toda la estrategia y así poder influir dentro de una entidad; y, finalmente, fomentar un equilibrio de prioridades operativas y de seguridad dentro de todo el conjunto de medidas de gestión de riesgos para cada entidad. Otra práctica a notar en el caso de México es la necesidad de que infraestructuras, entidades o actores relevantes con acceso a la principal red de comunicación financiera interbancaria cuenten con la figura de director de Seguridad de la Información (CISO) y un equipo de respuesta de seguridad cibernética que además esté coordinado con las autoridades pertinentes, en materia de protocolos de prevención y respuesta.

En el caso de Hong Kong, dicha jurisdicción lanzó desde hace un par de años la Iniciativa de Fortalecimiento de la Ciberseguridad (CFI, por sus siglas en inglés), que se fundamenta en tres pilares: a) un marco general para evaluar la seguridad cibernética, incluyendo elementos de examinación de riesgos inherentes, aspectos de madurez y una prueba de simulación de ataque cibernético basada en inteligencia (iCAST); b) un programa de desarrollo profesional en las entidades, que busca aumentar la oferta de profesionales de seguridad cibernética calificados y donde, por ejemplo, entes académicos han logrado desarrollar un esquema de certificación y un programa de capacitación para profesionales de la seguridad cibernética; y, finalmente, c) una plataforma de intercambio de información, denominada Cyber Intelligence Sharing Platform, que busca proporcionar una infraestructura efectiva para compartir inteligencia acerca de incidentes y donde la coordinación interinstitucional ha sido un aspecto fundamental en los ciberataques; siendo establecida por la HKMA junto con la Asociación de Bancos de HK. Algo que se puede destacar del caso de Hong Kong respecto de otros países es el hecho de que en sus prácticas se prima la exigencia para todas las entidades bajo el marco de regulación el requisito de integrarse a una red de inteligencia por el bien común del sistema financiero.

En el caso del Reino Unido, se cuenta con un marco de trabajo conocido como CBEST, que se ha apuntalado como un referente internacional guiado por el uso de inteligencia que se centra en validar la vulnerabilidad y la capacidad de recuperación del riesgo cibernético de una entidad o infraestructura, todo ello adoptando una postura en la que los objetivos probables y métodos de ataque son el principal elemento de análisis y seguimiento. Este marco es conducido por el banco central de ese país y cuenta además con elementos adicionales que fortalecen su imagen como referencia a nivel internacional, especialmente en materia de evaluación de capacidades de detección y respuesta que permiten establecer si los niveles de seguridad cibernética de las entidades, infraestructuras y agentes es proporcional a los riesgos cibernéticos que enfrenta. La posibilidad de que a nivel global este se convierta en un enfoque común no es muy clara, debido a elementos críticos con los que tiene que contar: personal y capacidad instalada para desempeñar las funciones de inteligencia, y porque también se hace indispensable poder validar regularmente en qué medida se tienen parámetros y medidas de calidad de la inteligencia cibernética.

En el caso de República Dominicana, en 2018 se emitió el Programa de Seguridad Cibernética y de la Información que el banco central y la agencia de supervisión financiera de ese país emplean como principal herramienta de trabajo para fomentar controles, políticas y medidas más rigurosas de control del riesgo cibernético, con un foco en la integridad y disponibilidad de información y servicios críticos para el sistema financiero. Este marco de trabajo es un enfoque mucho más tradicional en el que las entidades financieras están encargadas de asegurar una estructura de gobierno y medidas que les permitan ser acreditadas en el Programa (nacional) de Seguridad Cibernética. Se puede destacar que en este Programa se pone un énfasis especial en la criticidad de las infraestructuras de mercado, particularmente en el principal sistema interbancario de transferencia de fondos. Parte de este énfasis tiene que ver con la interconexión dentro del sistema financiero como una de las principales fuentes del riesgo tecnológico. Del mismo modo, el Programa busca que los aspectos de cultura institucional y la gestión de riesgos con terceras partes tenga un valor importante dentro de todas las medidas que puedan adoptar las entidades sujetas a cumplir con esta normativa.

Como se puede ver, este conjunto de prácticas domésticas son el reflejo de un interés incuestionable de las autoridades financieras de todo el mundo por encaminar al sistema financiero y sus participantes a un contexto en el que se asume y se comprende el riesgo cibernético como una importante y disruptiva fuente de riesgos para las economías.

La manera en la que cada jurisdicción aprovecha estas referencias y prácticas puede conducir a enfoques variados y una compleja manera de afrontar un fenómeno transfronterizo, global para ser más precisos, pero al menos constituyen experiencia tangible sobre maneras con las que se puede hacer frente a semejante desafío. Como parte de todo esto, nuevamente se debe mencionar que en vista de las dimensiones y naturaleza del fenómeno, hay un amplio margen para aumentar el nivel de cooperación y coordinación de autoridades de diferentes jurisdicciones con miras a lograr una convergencia de enfoques en un ámbito global.

Esfuerzos de cooperación internacional

Con el aumento de la probabilidad y posibles consecuencias de un evento de riesgo cibernético, han surgido múltiples iniciativas, grupos y nichos de cooperación internacional para tratar de abordar las implicaciones de este fenómeno transfronterizo. En muchos de los casos, lo que se ha buscado es tratar de armonizar los enfoques y estrategias que delinean las acciones en las entidades y en las autoridades para identificar, responder y aprender de ataques cibernéticos. En otros casos, se ha buscado establecer recomendaciones de orden general que aseguren un nivel mínimo de estructura a los planes y políticas operativas para enfrentar este tipo de riesgos, pero en un formato equiparable que fortalezca la respuesta y capacidad institucional de quienes adoptan este tipo de recomendaciones, y que a la vez les permita formar parte de un proceso de aprendizaje continuo.

En esta sección se presentan algunos de estos espacios y mecanismos de coordinación internacional, enfatizando su alcance, implicaciones y retos de implementación.

El marco de trabajo del G7 para la Ciberseguridad en el Sector Financiero

El G7[15] estableció un Grupo de Expertos Cibernéticos (CEG, por sus siglas en inglés) con el fin de facilitar la coordinación entre los miembros y desarrollar un “enfoque” del G7 sobre la ciberseguridad en el sector financiero de sus países integrantes. Gracias a este esfuerzo de coordinación, en 2016 se promulgaron un conjunto de recomendaciones no vinculantes para tratar de aglomerar aspectos clave para el establecimiento de un marco único de prácticas de ciberseguridad para entidades privadas y públicas del sector financiero.

A la par de este esfuerzo, el CEG del G7 continuó trabajando en el desarrollo de un marco de evaluación de estas recomendaciones y en identificar los riesgos cibernéticos a partir de la mayor presencia de terceras partes, así como en promover una mayor coordinación intersectorial. En 2018, el CEG también publicó lineamientos para promover la seguridad cibernética en terceras partes y un conjunto de lineamientos para pruebas de penetración basadas en amenazas.

Si bien, ninguna de estas recomendaciones tiene carácter vinculante, han sentado un importante antecedente a nivel de las principales economías avanzadas para promover mayores esfuerzos y herramientas de convergencia hacia un marco apropiado de atención del riesgo cibernético, tanto en el sistema financiero como entre instituciones oficiales y autoridades financieras.

Cuadro 1. Lineamientos fundamentales del G7 para la ciberseguridad en el sector financiero

Lineamiento 1: Estrategia y marco de ciberseguridad

Establecer y mantener una estrategia y un marco de ciberseguridad adaptados a los riesgos cibernéticos específicos y debidamente adaptados a normas y directrices internacionales, domésticas y de la industria.

Lineamiento 2: Gobernanza

Definir y facilitar el desempeño de funciones y responsabilidades para que el personal involucrado pueda implementar, gestionar y supervisar la eficacia de la estrategia y el marco de seguridad cibernética para asegurar la rendición de cuentas; y proporcionar los recursos y poderes adecuados, así como el acceso a los órganos de gobierno de su respectiva entidad o institución.

Lineamiento 3: Evaluación de riesgos y control

Identificar funciones, actividades, productos y servicios –incluyendo interconexiones, interdependencias y el papel de terceras partes– priorizando su importancia relativa y evaluando su respectivo nivel de riesgo. Al mismo tiempo, identificar e implementar controles –políticas, procedimientos y capacitación– para proteger y gestionar esos riesgos dentro del rango de tolerancia establecida por los órganos de gobierno de la entidad o institución.

Lineamiento 4: Seguimiento

Establecer procesos de seguimiento sistemático para detectar rápidamente incidentes cibernéticos y periódicamente evaluar la efectividad de los controles identificados, incluso a través de monitoreo de red, pruebas y auditorías.

Lineamiento 5: Respuesta

Oportunidad y capacidad para: a) evaluar la naturaleza, el alcance y el impacto de un incidente cibernético; b) contener el incidente y mitigar su impacto; c) notificar a las partes involucradas internas y externas (como la aplicación de la ley, reguladores y otras autoridades públicas, así como accionistas, proveedores de servicios de terceros y clientes según corresponda); y d) coordinar las actividades de respuesta conjunta según sea necesario.

Lineamiento 6: Recuperación

Restablecimiento de funciones de manera responsable, al tiempo que se favorece la remediación continua, incluso mediante: a) eliminar afectaciones remanentes del incidente; b) restaurar sistemas y datos a sus niveles de normalidad; c) identificar y mitigar todas las vulnerabilidades que fueron explotadas; d) remediar las vulnerabilidades para prevenir incidentes similares; y e) comunicar adecuadamente a nivel interno y externo sobre el proceso de recuperación.

Lineamiento 7: Intercambio de información

Participar en el intercambio de información oportuna y confiable con actores internos y externos que estén interesados e involucrados (incluyendo entidades privadas y autoridades públicas dentro y fuera del sector financiero) sobre amenazas, vulnerabilidades, incidentes y respuestas para mejorar las defensas, limitar los daños, aumentar la conciencia situacional y ampliar el aprendizaje.

Lineamiento 8: Aprendizaje continuo

Revisar la estrategia y el marco de seguridad cibernética periódicamente –gobernanza, evaluación de riesgos y control, seguimiento, respuesta, recuperación e intercambio de información– y cuando los eventos lo justifiquen, abordar novedades del riesgo cibernético, asignando recursos, identificando y remediando brechas e incorporando las lecciones aprendidas.

Fuente: *G7 Cyber Experts Group*

Otro aspecto importante de los esfuerzos que ha promovido el G7 a través del trabajo del CEG es que se ha elevado el nivel de conciencia sobre la coordinación internacional en un ámbito mucho más amplio y no únicamente entre economías avanzadas. Esto, a raíz de incidentes de carácter cibernético como el ocurrido con el banco central bangladesí (Bangladesh Bank) que llevó a la desviación de recursos por operaciones transmitidas vía SWIFT al Banco de la Reserva Federal de Nueva York. Con ello, se demostró que los frentes de acción del crimen cibernético van más allá de los grandes centros financieros internacionales y se requiere establecer mejores prácticas a nivel mundial para enfrentar el riesgo cibernético.

La agenda de Ciberseguridad del Financial Stability Board[16]

El Financial Stability Board (FSB), o Consejo de Estabilidad Financiera, fue establecido en 2009 como un órgano de coordinación internacional encargado de promover la reforma de la regulación y supervisión financiera internacional a partir de la crisis financiera global.[17]

La importancia del FSB radica en que su agenda es fundamentalmente establecida por las veinte principales economías del mundo, o lo que se denomina G20, y que engloba economías avanzadas y también economías emergentes, cuyo papel en la discusión y tratamiento de temas de carácter internacional es clave para abarcar las preocupaciones tanto de sistemas financieros como el del Reino Unido, hasta de aquellos en economías como la de Indonesia o México; es decir, incorporar las vulnerabilidades que afectan al sistema financiero a nivel mundial y adoptar medidas que podrían ser útiles para la estabilidad financiera internacional, teniendo presente la visión de las economías emergentes. De esta manera, el G20 representa en mejor medida que el G7 las realidades y circunstancias de las distintas economías a nivel mundial, y por ello, en el caso del riesgo cibernético, la atención que comenzó a brindar el FSB ha sido un paso importante en la coordinación y cooperación internacional.

En octubre de 2017, el FSB divulgó un informe que revisa las prácticas y normativa de ciberseguridad en los países miembros del G20, con el fin de identificar aspectos que pueden resultar clave en materia de cooperación transfronteriza. De acuerdo con este informe, por ejemplo, el 75% de países considerados en el estudio está tomando como referencia el Guidance on Cyber Resilience for Financial Market Infrastructures publicado por el Comité de Pagos e Infraestructuras de Mercado (CPMI, por sus siglas en inglés) y la Organización Internacional de Comisiones de Valores (IOSCO) en 2016; por otra parte, 68% de los países están certificándose con el estándar ISO/IEC 27000, adoptando con ello directrices para la gestión de riesgos informáticos y la constitución de un Sistema de Gestión de Seguridad de la Información (SGSI); finalmente, un porcentaje muy similar está tomando como punto de partida el marco del NIST que surgió en 2014 en Estados Unidos y que estaba originalmente pensado para infraestructuras críticas pero que, al ofrecer un enfoque integral, distintas entidades y organizaciones lo han visto como una herramienta útil para mejorar su capacidad de prevenir, detectar y responder a los ciberataques.

También, gracias a este informe fue posible observar que las autoridades de todo el mundo vienen tomando distintos enfoques y medidas regulatorias y de supervisión abocadas a la mitigación del riesgo cibernético, así como medidas para una respuesta y recuperación efectiva por parte de las instituciones financieras.

El FSB continuó su trabajo de coordinación internacional mediante la creación de un glosario de términos asociados con la seguridad cibernética, en el que se incluyen más de 50 términos de uso cada vez más común entre las autoridades financieras y las entidades del sistema financiero, a nivel doméstico y también a nivel internacional. El glosario, o Cyber Lexicon, busca armonizar el trabajo y los esfuerzos para abordar el riesgo cibernético, mediante la provisión de un entendimiento común intersectorial de

conceptos clave alrededor de la seguridad cibernética, así como facilitar en el futuro cercano un marco de intercambio de información, evaluación y seguimiento sobre las vulnerabilidades relacionadas con incidentes de carácter cibernético.

Ambas piezas de información, el informe sobre prácticas regulatorias y de supervisión y el glosario son piezas fundamentales de la actual agenda de trabajo del FSB en materia de seguridad cibernética y como tales han proporcionado orientación importante a nivel internacional para tener una mejor comprensión y conocimiento del riesgo cibernético. Por ejemplo, ahora es posible concluir que en vista de la naturaleza compleja y evolutiva de las innovaciones financieras y su expresión en términos de riesgos cibernéticos, las autoridades domésticas e internacionales muestran una inclinación hacia el establecimiento de marcos de regulación y supervisión basada en principios, que además sean proporcionales a la naturaleza, el tamaño, la complejidad y el perfil de riesgos inherentes al tipo de entidad, plataforma o servicio que se trate; en esa misma línea, también es posible ver que para alcanzar un marco de este tipo que sea confiable y a la vez capaz de adaptarse a la situación cambiante, es necesario que las entidades financieras, instituciones oficiales, autoridades domésticas y organismos multilaterales, concuerden todos en prácticas confiables y —en lo posible— armonizadas de identificación, evaluación y mitigación de riesgos, para que con ello se pueda determinar de manera más acertada el diseño del marco de regulación y supervisión desde la óptica de la seguridad cibernética. A la par, también se ha identificado que, para fortalecer este tipo de marco de trabajo, es conveniente identificar y actualizar los requisitos (mínimos) de seguridad cibernética en todo el sistema financiero y así proveer de suficientes elementos de orientación a las entidades financieras y otras partes involucradas en el sistema financiero. Otro ejemplo es que, gracias a estos esfuerzos del FSB, es posible contar con la visión del sector privado (entidades financieras, infraestructuras y plataformas de mercado) que aboga por la adopción de un enfoque estratégico, coherente y proactivo a nivel mundial, enfatizando el buen gobierno y, sobre todo, esquemas regulatorios armonizados.

Otra vía con la que el FSB ha continuado sus esfuerzos de coordinación internacional son los grupos consultivos regionales (RCG, por sus siglas en inglés). Actualmente, el FSB cuenta con seis RCG, incluido uno para América, con los que busca ampliar su ámbito de divulgación y aplicación más allá del G20, de esta forma, a través de los RCG, el FSB también ha promovido una mayor concientización y necesidad de mecanismos más formales de cooperación a nivel mundial en materia de seguridad cibernética. Esto es un elemento clave para el trabajo en curso del FSB para promulgar un conjunto de prácticas relacionadas con la respuesta y recuperación efectivas ante incidentes cibernéticos[18]; sea a través de los RCG o de una coordinación global promovida por el FSB junto con otros organismos y grupos internacionales, como puede ser el Comité de Supervisión Bancaria de Basilea (BCBS) u otros que tengan un papel relevante en promover la aplicación de estas prácticas recomendadas.

El marco de trabajo del Comité de Pagos e Infraestructuras de Mercado

El Comité de Pagos e Infraestructuras de Mercado (CPMI, por sus siglas en inglés) es un organismo que establece estándares (standard setting body) que se formó a inicios de los noventa, con el fin de analizar el avance y las cuestiones clave sobre el funcionamiento de lo que en aquel momento representaba el sistema de pagos, esquemas de compensación interbancaria. Desde entonces, el CPMI ha contribuido significativamente con la comunidad financiera internacional (sectores público y privado) a promover mejores prácticas sobre la seguridad y eficiencia de la infraestructura del sistema financiero.

Actualmente, el CPMI está compuesto por 27 de las principales economías del mundo y en materia de seguridad cibernética ha hecho importantes contribuciones para apoyar la cooperación internacional y la adopción de estándares que fortalezcan las prácticas contra el crimen cibernético en el sistema financiero y en las propias infraestructuras de mercado.

Particularmente, en 2016, el CPMI publicó una guía para el fortalecimiento de la seguridad cibernética dentro de las principales infraestructuras del mercado financiero, incluidos los sistemas de pago de importancia sistémica. La guía también es pertinente para las autoridades de regulación y supervisión financiera en el desempeño de sus responsabilidades microprudenciales. En general, la guía se propone como una orientación para que todas las autoridades financieras relevantes promuevan su uso de acuerdo con las leyes y regulaciones aplicables en cada país, reconociendo que es importante adaptarla según el marco institucional existente[19]. El enfoque propuesto por el CPMI ha sido adoptado por sus 27 miembros, y a través de un ámbito de cooperación internacional como el que promueven instituciones como el CEMLA en América Latina y el Caribe, el SEACEN en Asia o el Banco Central Europeo en Europa también ha sido posible ampliar su adopción.

De acuerdo con el FSB, este marco de trabajo del CPMI se ha convertido en un referente internacional relevante, incluso más allá de la esfera de infraestructuras financieras, para extenderse a cuestiones prudenciales, aplicables a las prácticas de riesgo cibernético en entidades financieras, al menos en lo que respecta al uso y acceso a infraestructuras de mercado. De esta manera se ha logrado una importante contribución a las medidas supervisoras dentro del sistema financiero de países que las vienen adoptando.

Es importante señalar que luego de la publicación de esta guía, el CPMI en concordancia con otros organismos internacionales, incluida la IOSCO, pero otros como el Banco Mundial y, en general, la comunidad financiera internacional han puesto un foco especial en buscar que este marco de referencia se considere un elemento imprescindible para alcanzar una regulación y estabilidad financiera dentro de cada economía, buscando así una armonización de prácticas y estándares.

Si bien esta guía constituyó también un avance considerable en materia de coordinación a nivel internacional, con la creciente y compleja utilización de información de los clientes y usuarios de servicios de pago, y la mayor dependencia a tecnologías informáticas, el crimen cibernético también se especializó y comenzó a centrar sus ataques en infraestructuras del sistema financiero que son críticas. El ejemplo más claro de ello fue el robo al Bangladesh Bank, el banco central bangladesí, que fue vulnerado y utilizado para un robo multimillonario que involucró a la red de mensajería SWIFT y que tenía como aparente contraparte a un banco del Sistema de la Reserva Federal; luego acontecieron otros incidentes de conocimiento global, como fue el ataque a las plataformas de comunicación que el sistema financiero mexicano utilizaba para conectarse al sistema interbancario de fondos, entre otros ataques de naturaleza similar y que se podrían clasificar como APT38.

Es a partir de la aparición de este tipo de incidentes que nuevamente el CPMI, en representación de la comunidad financiera internacional especializada en infraestructuras financieras, dio a conocer una estrategia enfocada en reducir el riesgo cibernético en los puntos de acceso de las plataformas e infraestructuras de mercado que son de importancia sistémica, incluyendo redes financieras y de mensajería como SWIFT a las que prácticamente todas las entidades financieras de cada país tienen acceso. Dicha estrategia fue publicada en mayo de 2018 y es, en términos generales, un llamado al sistema financiero global a redoblar esfuerzos para contrarrestar al crimen cibernético, con acciones palpables, integrales y efectivas que se apoyen en un diálogo entre participantes de la industria financiera, el intercambio de información útil entre distintos países o sistemas e infraestructuras transfronterizas, y mediante el uso de un enfoque analítico y una terminología común que evite una mala interpretación de objetivos, acciones y resultados esperados.

Este desarrollo del CPMI también marcó una nueva etapa de la coordinación y cooperación internacional contra el crimen cibernético, no solo porque se acompañó de la publicación del programa de seguridad del cliente Customer Security Programme (CSP, por sus siglas en inglés) de SWIFT[20], sino porque el CPMI

conjuntamente con el FSB solicitaron a todos los bancos centrales del mundo, la adhesión a esta estrategia para con ello alcanzar un enfoque holístico y coordinado, con el fin último de que todos los participantes de la industria, incluyendo autoridades y entidades financieras, infraestructuras, proveedores y otras terceras partes, internalicen las acciones pertinentes de seguridad cibernética y así contribuyan a mitigar vulnerabilidades en sus propios perímetros de operación, conexión y comunicación dentro de todo el sistema.

En adelante, es de esperarse que el CPMI continúe desempeñando un papel importante en la coordinación de esfuerzos contra el crimen cibernético, en particular desde la óptica y la comunidad de bancos centrales y autoridades financieras relevantes para los sistemas de pago y las infraestructuras de mercado.

El marco de trabajo del Eurosistema y el Banco Central Europeo

El Banco Central Europeo (BCE) es el banco central de los diecinueve países que forman la unión monetaria de Europa y que se denomina también como Eurosistema. El BCE está encargado, entre otros objetivos, de preservar la estabilidad financiera en esa región, en coordinación con los bancos centrales nacionales del Eurosistema.

En materia de riesgo cibernético, el BCE ha desarrollado un marco de trabajo enfocado en garantizar la protección, disponibilidad e integridad de la información en el sistema financiero, particularmente de las economías que lo componen. Gracias a que el BCE responde a la necesidad de tener una arquitectura financiera regional, en este caso para el Eurosistema, los esfuerzos y la vinculación normativa que se han emprendido recientemente contribuyen a que las potenciales consecuencias y efectos del riesgo cibernético se mitiguen.

El marco de trabajo del BCE en cuestiones cibernéticas se puede desagregar en tres componentes:

- Plan de acción sobre resiliencia cibernética para infraestructuras de mercado (APCR)
- Expectativas de supervisión sobre resiliencia cibernética (CROE)
- Iniciativa de hacking ético basada en inteligencia de amenazas (TIBER-UE)

Estos tres pilares son la base para la estrategia contra ataques dentro de los bancos centrales nacionales de Europa, y que se extienden al sistema financiero de esa región. Se puede destacar que para la implementación del APCR, el BCE contó con un órgano de gobierno, denominado Consejo de Infraestructuras Financieras, para poner en funcionamiento dicho plan en 2017. La importancia del APCR radica en el grado de coordinación que se alcanzó con su lanzamiento, poniendo atención especial a aspectos de gobernanza y organizacionales, con tal de asegurar que las medidas de detección, prevención, respuesta y recuperación estuvieran plenamente identificadas, soportadas y cubiertas por los países miembros del Eurosistema. Asimismo, el APCR es constantemente actualizado por el BCE, con miras a permanecer vigente como la principal línea de defensa contra el crimen cibernético. Por ejemplo, promoviendo la mejora de las actividades de monitoreo y registro de incidentes en la principal infraestructura tecnológica, así como reforzando las actividades de prueba de los controles de seguridad, como es el caso de la formación y el funcionamiento de equipos rojos (para ejercicios de penetración y pruebas basadas en escenarios).

Si bien el APCR es el eje rector del marco del BCE, el TIBER-UE, como se acaba de mencionar, es una respuesta coordinada muy concreta dentro del Eurosistema para contrarrestar el riesgo cibernético. Esta iniciativa de hacking ético basados en inteligencia de amenazas contribuye a identificar de manera más expedita cambios importantes en tácticas, técnicas y procedimientos de criminales cibernéticos; de esta manera, el BCE cuenta con el respaldo de un equipo experimentado que permite elevar el nivel de coordinación dentro de la región, sometiendo a infraestructuras y funciones críticas comunes a fortalecer sus capacidades de protección, detección y respuesta. Finalmente, el CROE se ha constituido como un elemento adicional al marco de trabajo del BCE que establece un mínimo de acciones y medidas que las autoridades esperan que el sistema financiero y sus infraestructuras de apoyo adopten; ello como parte de la guía promovida en 2016 por el CPMI. Los elementos centrales del CROE se pueden resumir en lo siguiente:

- Orientar a las infraestructuras de mercado sobre la puesta en marcha de un marco de seguridad cibernética basado en acciones sujetas a una mejora constante a lo largo del tiempo.

- Proporcionar a los supervisores financieros y a los bancos centrales expectativas claras para evaluar las infraestructuras (y a sus respectivos participantes) en términos de los controles y políticas de seguridad cibernética.

- Sentar la base para un proceso abierto y verificable de evaluación de las medidas en curso, entre las infraestructuras y sus respectivos supervisores.

Un aspecto que merece mención especial, no solo a nivel europeo, es que la industria financiera ha manifestado que el CROE puede considerarse un mecanismo de aplicación y cumplimiento dentro de las entidades financieras (con fines de supervisión) y otras partes relevantes de los mercados y el sistema financiero en general. Esto, porque en gran medida esta orientación del BCE establece parámetros de prescriptividad de las expectativas entre los supervisores y las entidades e infraestructuras; así como permitir tener un parámetro armonizado de mejoramiento de las medidas para contrarrestar el riesgo cibernético en distintos niveles de madurez y adopción; y, finalmente, porque también facilita tener un ejercicio de evaluación por parte de los supervisores con expectativas claras para las principales partes del ecosistema financiero.

En este contexto, la supervisión financiera que el BCE desempeña a través de su Mecanismo Único de Supervisión (MUS), basándose en estos pilares, ha implementado un marco de información de incidentes cibernéticos, de tal manera que las principales entidades financieras (Global Systemically Important Banks, o G-SIBS) están obligadas a reportar incidentes cibernéticos significativos apenas son detectados; ello, con el fin de permitir que los supervisores puedan identificar y dar seguimiento a la evolución del crimen cibernético, así como poder reaccionar de manera más coordinada y expedita en casos de incidentes inminentes. A través de un conocimiento más profundo y de primera mano de riesgos cibernéticos. Es de destacar que, gracias a estos esfuerzos, los 19 países miembros del Eurosistema han alcanzado un nivel único de supervisión de riesgos informáticos que en gran medida se pueden ver como una mejor práctica a nivel internacional, tanto por el nivel de coordinación y cooperación, como por el desarrollo de un marco efectivo para atender esta nueva dimensión de riesgos en el sistema financiero. Por ejemplo, se pueden mencionar las prácticas de supervisión continua extra situ, revisiones temáticas y horizontales de áreas de enfoque (riesgo cibernético, calidad de datos, etc.), inspecciones in situ (en áreas de riesgo informático y cibernético). Por último, se está trabajando para emitir directrices sobre la gestión del riesgo cibernético, dentro de las propias entidades financieras.

Un último aspecto que se podría señalar de los esfuerzos de coordinación regional en el Eurosistema es la colaboración que existe entre el Parlamento Europeo, el Consejo y la Comisión Europea, que en

conjunto con el BCE ha permitido poner en funcionamiento un Equipo de Respuesta a Emergencias Informáticas (CERT-UE) que sirve de mecanismo de alerta para quienes son miembros de este equipo acerca de nuevas amenazas.

El Grupo de Trabajo de Resiliencia Operativa del Comité de Supervisión Bancaria de Basilea

El Comité de Supervisión Bancaria de Basilea (BCBS) es un órgano internacional de coordinación y emisión de recomendaciones y estándares internacionales para la regulación y supervisión financiera. El BCBS es hospedado por el BIS y su composición está dada por las autoridades de supervisión bancaria de todo el mundo y su principal misión es fortalecer la solidez de los sistemas financieros a través del diálogo internacional y la promulgación de estándares que contribuyan a su misión. El BCBS es ampliamente reconocido en la comunidad financiera internacional por el establecimiento del Acuerdo de Capital de Basilea (Basilea I) y sus sucesivas reformas, y por haberse consolidado como el centro de la regulación financiera mundial. A ello se tiene que destacar que, gracias a una creciente colaboración y coordinación internacional, ha sido posible que distintas normas y estándares emitidos por este comité, se adopten y pongan en práctica a nivel doméstico y a nivel global, aunque claramente con diferencias notables de enfoque y de alcance, en función de la aplicabilidad de sus normas dentro de cada jurisdicción.

En este marco, el BCBS reconoció en 2018 la importancia de estudiar el estado de la resiliencia operativa más allá del alcance de la gestión del riesgo operacional y del riesgo cibernético, y para ello estableció el Grupo de Trabajo de Resiliencia Operacional (ORG, por sus siglas en inglés) buscando contribuir con otros esfuerzos de carácter internacional al tratamiento de este fenómeno en una escala transfronteriza y coordinada. Adicionalmente, el BCBS como parte de su proceso de reforma poscrisis, en 2016 presentó una revisión, Principios para la Gestión del Riesgo Operacional, que se enfocó en incorporar aspectos y lecciones de la CFG, incluyendo algunas cuestiones asociadas con el riesgo cibernético. Estos Principios establecen unas expectativas comunes que son de aplicación a entidades financieras de importancia sistémica, pero dado el papel que el BCBS tiene a nivel de regulación financiera internacional, constituyen un referente más para orientar la implementación de políticas, procedimientos y prácticas para administrar el riesgo operacional y cibernético; además, favoreciendo que las medidas que adopte cada entidad, infraestructura o actor relevante reflejen la complejidad (interconectividad), exposición y nivel de riesgo que represente a nivel macro.

Como es de esperarse, estos Principios implican un nivel de complejidad y costos financieros elevados, por lo que su adopción a nivel internacional en el corto plazo puede verse limitada, dado que también, por otro lado, la industria está encarando nuevos retos operacionales ante la llegada de nuevas tecnologías financieras que suponen un cambio de paradigma. Por ello, se puede anticipar que el progreso en la implementación de los principios varíe significativamente entre un país y otro.

Asimismo, es de esperarse que el BCBS por intermedio del ORG u otros canales continúe monitoreando la evolución del riesgo cibernético a nivel global y actúe en concordancia y tiempo, tal vez en coordinación con otros actores como el FSB, para apoyar los esfuerzos de coordinación internacional en la batalla contra este fenómeno.

Retos para la coordinación internacional

Tal como señala el FSB, tras la CFG, la serie de reformas financieras lideradas por el G20 sirvieron para cubrir los espacios que la regulación no pudo anticipar previamente. En ese marco, la coordinación y cooperación internacional fueron instrumentales en implementar los cambios que exigió la reforma financiera a nivel internacional.

No obstante, y quizás mucho más que antes de la CFG, el mundo financiero se está transformando gracias a la llegada de nuevas tecnologías, y es de suponer que esto traiga implicaciones para la seguridad cibernética. Por ello, hacia futuro, sería deseable que se fortalezcan los mecanismos de cooperación internacional.

El crimen cibernético sigue reinventándose de manera considerable, mostrando nuevas dimensiones de ataque y de objetivos. Si bien las prácticas existentes a nivel doméstico e internacional constituyen un importante referente para que se consoliden prácticas de seguridad cibernética a nivel global, con alta probabilidad, será necesario que las autoridades, entidades, infraestructuras y actores relevantes del sector financiero se mantengan preparados y actualizados para responder de manera efectiva ante este fenómeno. En ese sentido, la comunidad financiera internacional tiene por delante el reto de ir cerrando brechas conceptuales y de atención del riesgo cibernético, especialmente en el área de estándares y recomendaciones internacionales. Por ejemplo, asegurar que cuestiones de identificación, calibración y diseño de escenarios de riesgos sea consistente (o al menos comparable) entre jurisdicciones, para que las autoridades y las propias entidades e infraestructuras financieras sean capaces de compartir información y poder reaccionar de manera coordinada ante incidentes que sobrepasan las fronteras de sus propias economías. Los aspectos que mínimamente deberán ser revisados en la actual lista de estándares internacionales para el tratamiento del riesgo cibernético incluyen, entre otros, los siguientes:

- Gobernanza y marco general de trabajo
- Análisis y evaluación de riesgos
- Confidencialidad, integridad y disponibilidad de la información
- Controles de seguridad y prevención de incidentes
- Habilidades y capacitación para abordar los eventos de riesgo
- Seguimiento, marco de pruebas y de control interno
- Capacidad y mecanismos de respuesta
- Comunicación efectiva e intercambio de información entre agentes relevantes internos y externos
- Supervisión de terceras partes y de los lazos de interconexión e interdependencia
- Cultura y aprendizaje de las personas.

Si la comunidad financiera internacional es capaz de identificar las diferencias que se han presentado en el desarrollo de estos referentes, será relativamente sencillo dedicar esfuerzos nuevos en coordinarse para lograr que surja un entendimiento común de los principios (estandartes o normas) que puedan sentar las bases de un enfoque estandarizado global para enfrentar el riesgo cibernético; el Acuerdo de Capital de Basilea (hoy en día, Basilea III) es un ejemplo del grado de coordinación que se necesita a nivel internacional en cuestión del riesgo cibernético. La creación de un órgano que pueda desempeñar ese papel no es una tarea que vaya a resultar sencilla, pero sería un elemento que seguramente sumaría a dichos esfuerzos. Y, aun así, es importante reconocer que —como en otros ámbitos de cooperación internacional— la manera en la que se adopten los principios o estándares (cualesquiera que sean) en

cada jurisdicción va a depender de la configuración legal, institucional y operativa del sistema financiero de cada país; al respecto, la armonización podría buscarse desde el papel de las autoridades en establecer los requisitos y condiciones sobre los que se tienen que desarrollar las medidas y estrategias en cada entidad, infraestructura o agente relevante.

Para concluir y de cara al futuro, no es previsible que el riesgo cibernético vaya a desaparecer, por lo que va a ser importante aprovechar los recursos y la experiencia que se tengan, y dentro de ellos, los mecanismos de coordinación internacional para favorecer que cada parte (de un todo) contribuya a asegurar los distintos niveles y perímetros de control de este tipo de riesgo son una pieza fundamental.

Referencias

- Banco de México. Estrategia de Ciberseguridad del Banco de México. Octubre 2018.
- Bank of England. CBEST framework. June 2013.
- Basel Committee on Banking Supervision. Cyber-resilience: range of practices. December 2018.
- Committee on Payments and Market Infrastructures and International Organization of Securities Commissions. Guidance on cyber resilience for financial market infrastructures, June 2016.
- Committee on Payments and Market Infrastructures. Reducing the risk of wholesale payments fraud related to endpoint security. May 2018.
- European Central Bank. TIBER-EU framework. May 2018.
- European Central Bank. Cyber resilience oversight expectations for financial market infrastructures. December 2018.
- Financial Stability Board. FSB 2017 workplan. November 2016.
- Financial Stability Board. Financial stability implications from fintech: supervisory and regulatory issues that merit authorities' attention, June 2017.
- Financial Stability Board. Cyber Lexicon. November 2018.
- Financial Stability Institute. Regulatory approaches to enhance banks' cyber-security frameworks. August 2017.
- G-7. Fundamental Elements of Cybersecurity for the Financial Sector. October 2016
- G-7. Fundamental Elements for Effective Assessment of Cybersecurity in the Financial Sector. October 2017.
- Hong Kong Monetary Authority. Cybersecurity Fortification Initiative, May 2016.
- Superintendencia de Bancos. Reglamento de seguridad cibernética de la información. Noviembre 2018.

Tendencias del fraude cibernético y mejores prácticas en el sector financiero global

Adam Palmer, Gilberto Martins de Almeida

Antecedentes

La conectividad global del ciberespacio pone a disposición de todos una plataforma para favorecer que la actividad de fraude se propague más rápidamente y fácilmente por todas las fronteras geográficas. Este problema de no contar con fronteras se evidenció con el contagio de ataques de jackpotting en cajeros automáticos en 2018. Se observó que estos ataques, utilizando metodologías similares, se propagaron tanto en Europa como en América Latina. Los ataques utilizaron *malware* similar para explotar sistemas obsoletos en máquinas de cajeros automáticos, lo que provocó el vaciado ilegal de los contenidos de algunas de estas máquinas en Alemania, Brasil y México y ser recolectados físicamente por los ladrones.

Otro ejemplo de amenaza de fraude cibernético global sin fronteras se refiere a los ataques denunciados contra el sistema de pago SWIFT en México, Bangladesh, Vietnam y Ecuador entre 2015 y 2018. Así se demuestra cómo el ciberespacio permite que los delincuentes cometan fraude contra organizaciones y sistemas establecidos globalmente. Mediante el uso de la tecnología cibernética, los delincuentes pueden desplazarse fácilmente a través de las fronteras nacionales o difundir rápidamente sus técnicas de explotación.

Este capítulo se centra en América Latina, así el problema de la ciberseguridad se entienda como un desafío global. Esto lo ha reconocido el grupo de investigación Celent en un informe reciente que indicó que el 82% de los Tesoreros a nivel mundial consideran la seguridad cibernética su principal desvelo en seguridad. Todavía, sin embargo, aunque hay avances en la conciencia de la situación, la preparación viene rezagada de la conciencia. El mismo informe señaló que:

- El 70% de las organizaciones no han desarrollado un plan de respuesta a incidentes cibernéticos.
- El 46% de las organizaciones no han implementado o mejorado su capacitación sobre concienciación de la suplantación de identidad (*phishing*) para empleados en los últimos 12 a 24 meses.
- El 43% de las organizaciones carecían de responsabilidad a nivel de la junta directiva para la revisión y gestión del riesgo cibernético.
- El 37% de las organizaciones aún no han estimado el impacto financiero de un ataque cibernético.
- El 34% de las organizaciones no evalúa a sus proveedores o clientes en riesgo cibernético.

Resumen de la respuesta del sector de servicios financieros al riesgo de fraude cibernético

La respuesta de la comunidad de servicios financieros a la amenaza del fraude cibernético está mejorando. Hay que anotar que las respuestas en el pasado reciente habían sido fragmentadas, reactivas y, a veces, carecientes de una estrategia integrada de gestión de riesgos del sector. Las prácticas fragmentadas se caracterizaban por la falta de estándares y mejores prácticas comunes para las organizaciones, un limitado intercambio de información sobre eventos de fraude, y modelos organizativos inconsistentes que no lograban armonizar la capacidad entre las organizaciones globales. Con demasiada frecuencia se abordaron las brechas en los controles de seguridad después de ocurrir los incidentes. Además, las tasas de detección de fraude, en algunos tipos de fraude cibernético, fueron muy lentas.

Actualmente se están implementando soluciones para atender muchos de los problemas anteriores. Las soluciones realizadas incluyen la integración de equipos de fraude, de blanqueo de capitales y de riesgo cibernético para lograr una visión integral del riesgo. Se está optimizando la detección, mediante el uso del análisis de datos grandes. La inteligencia artificial (IA) se está utilizando para identificar los indicadores de fraude más rápidamente. Las firmas de servicios financieros también han comenzado a realizar una revisión proactiva, de manera más regular, de los controles de prevención, detección y respuesta para asegurar que se implementen controles tanto apropiados como efectivos.

El sector de servicios financieros también ha reconocido la urgencia de contar con un enfoque integrado de gestión del riesgo operacional. Lo anterior ha llevado al aumento de la integración interna del fraude con otros grupos de riesgo y seguridad. Esta convergencia está diseñada para aprovechar las capacidades internas contra el riesgo y lograr un modelo de gestión de riesgo operacional más holístico.

Las partes interesadas externas tanto en el gobierno como en la industria también han mejorado el acompañamiento y la cooperación contra el fraude. Asociaciones público-privadas ahora desempeñan un papel transcendental en el aumento de la resistencia al fraude cibernético, al crear conciencia sobre las amenazas y al preparar el apoyo adecuado para lograr una respuesta efectiva. Un elemento crítico del desarrollo de capacidades contra el fraude cibernético es la capacidad de incorporar la inteligencia de amenazas, o información procesable, a una defensa organizacional general. El uso de la inteligencia es fundamental para tomar decisiones informadas sobre el riesgo, en temas de amenazas. Las áreas principales de la cooperación para la inteligencia de amenazas cibernéticas son actualmente:

- Asociaciones entre agentes del orden público (que incluyen informes, prevención, disuasión, interrupción, investigación y apoyo a las víctimas).

- Cooperación con terceros, incluida la industria (los ejemplos son campañas de sensibilización, promoción de la privacidad por diseño, seguridad por defecto y privacidad por defecto y desarrollo de herramientas).

- Canales de comunicación para el intercambio seguro y legal de información e inteligencia con socios relevantes.

Cuando se trata de detectar y prevenir el fraude cibernético, a menudo se usa el cliché de "se necesita una red para derrotar a una red". Dado el carácter sin fronteras y asimétrico, el volumen, el nivel de sofisticación y el impacto financiero de estos ataques, la cooperación de todas las partes interesadas a nivel nacional e internacional es la clave para la resiliencia.

Un ejemplo de la mejora de las plataformas de intercambio de inteligencia de las partes interesadas es la huella global ampliada del Centro de intercambio y análisis de información de servicios financieros (FS-ISAC, por sus siglas en inglés). El FS-ISAC ahora ha expandido sus operaciones de Norteamérica a tanto Europa como Latinoamérica. La presencia de esta importante organización de intercambio de inteligencia sobre amenazas de la industria promete entregar una capacidad de intercambio de información y coordinación más sólida por todo el sector. El FS-ISAC es un recurso global de la industria financiera para el análisis y el intercambio de inteligencia cibernética. Lanzado en 1999, FS-ISAC fue establecido por el sector de servicios financieros de EE. UU. en respuesta a la política del gobierno estadounidense que definía que los sectores público y privado de ese país debían compartir información sobre amenazas y vulnerabilidades físicas y de seguridad cibernética para ayudar a proteger la infraestructura crítica de EE. UU. Si bien el FS-ISAC siempre ha trabajado con miembros bancarios que cuentan con operaciones en todo el mundo, a principios de 2013 FS-ISAC amplió su estatuto para incluir el compartir información entre empresas de servicios financieros de todo el mundo. El FS-ISAC ahora ofrece una capacidad de intercambio de información anónima en toda la industria global de servicios financieros y así mejora la capacidad de detectar cualquier indicador de fraude y de compartir alertas con otras firmas financieras.

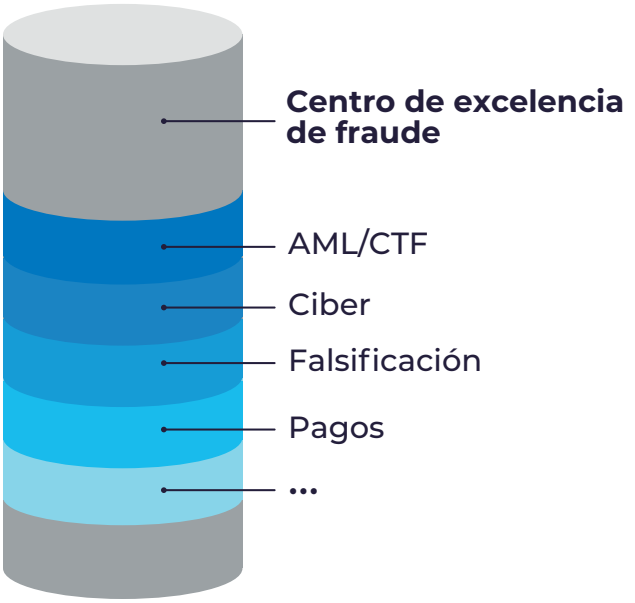
Modelos operativos del sector de servicios financieros para combatir el fraude cibernético

Las empresas de servicios financieros están desarrollando nuevos modelos operativos y plataformas para combatir el fraude cibernético. El objetivo es pasar del modelado básico de datos y grupos de riesgo independientes, al análisis inteligente de la información que apoya tanto la prevención como la detección rápida de fraudes. Las empresas están desarrollando capacidades para permitir el análisis de datos agregados y las correlaciones entre los datos cibernéticos y los datos de fraude. Esto soporta mecanismos de alerta mejorados y automatización de procesos rutinarios. Se puede usar el análisis de datos para identificar la "información desencadenante" que indica fraude o para distinguir el fraude potencial de la actividad normal. También se está facilitando el control mejorado de las identidades de los usuarios mediante el uso de técnicas de identificación biométrica. El objetivo subyacente de estas gestiones es crear una experiencia para el cliente que sea rápida, no onerosa y eficaz para confirmar la identidad del cliente y evitar transacciones fraudulentas.

Algunas empresas financieras ahora también están desarrollando Centros de Fusión de Fraude Cibernético. Las empresas están mejorando su modelo interno de silo actual, desde una estructura plana con departamentos independientes como:

- Invertigaciones cibernéticas
- Invertigaciones de seguridad física
- Invertigaciones de equipo inteligencia
- Invertigaciones blanqueo capital
- Invertigaciones auditoria interna

Esto se está convirtiendo en un modelo de centro de fusión integrado holístico como se ilustra en:



La estrategia de gestión de riesgos de fraude debe continuar evolucionando de modo que pueda abordar futuras amenazas desconocidas y lograr una mejor rendición de cuentas. La estrategia permitirá la supervisión holística de la gestión del fraude y la capacidad de control. El objetivo de los nuevos modelos operativos integrados es desarrollar una gestión de fraudes que sea:

1.) Preventiva y detective.

2.) Personalizada, pero integrada con datos compartidos.

3.) Operativa sin silos a través de organizaciones y geografías.

4.) Con forme a las mejores prácticas, para mejorar la mitigación con un impacto residual mínimo en la experiencia del cliente.

Cada una de las 3 líneas de defensa tiene un rol único en la implementación de un programa eficaz contra el fraude. La segunda línea de defensa debe establecer una gobernanza adecuada, desarrollar un perfil de riesgo con una supervisión independiente efectiva, informar sobre los principales riesgos de fraude, informar sobre eventos relevantes e infracciones del apetito de riesgo, y desafiar el Programa de Gestión de Fraude core 1 LoD. La primera línea de defensa debe tener responsabilidad de primera línea de identificación y evaluación del riesgo de fraude, desarrollo e implementación de un programa de gestión de fraudes (planes de mitigación para mejorar la gestión de riesgos de fraude clave), participación en la gestión de fraudes y definición de políticas y procedimientos para la gestión general de riesgos de fraude.

Tácticas, técnicas y procedimientos (TTP) relacionados con el fraude cibernético.

Las tácticas, técnicas y procedimientos (TTP, por sus siglas en inglés) utilizados para cometer fraudes cibernéticos incluyen, pero no se limitan a, ingeniería social, *phishing* y ataques de *malware*. Un informe reciente sobre un grupo de delitos financieros ofrece un ejemplo de ataques cibernéticos avanzados, utilizados para cometer fraudes. El grupo delictivo buscaba sistemáticamente información financiera en los sectores biomédico y farmacéutico. El grupo utilizaba correos electrónicos personalizados y sofisticados para atraer a las víctimas, que incluían a directores generales, directores financieros, científicos investigativos y abogados, y lograr que entregaran sus credenciales de correo electrónico. Luego, los atacantes se insertaban en las cadenas de correo electrónico, accediendo a información privilegiada y sensible al mercado que impactaba significativamente el valor de mercado de las compañías objetivo. Los ataques tuvieron éxito, sin tener que usar ningún *malware*, solo basándose en que los usuarios, sin saberlo, usan sus credenciales de correo electrónico en sistemas que ya se encontraban bajo el control del atacante. La falta de autenticación de dos factores en los sistemas de las víctimas que eran el blanco hizo que estos ataques fueran sencillos, pero altamente efectivos y les permitieron a los delincuentes obtener información privilegiada valiosa sobre las compañías objetivo.

Otro ejemplo de fraude cibernético fue reportado recientemente cuando unos atacantes usaron credenciales robadas para acceder a la infraestructura de red privada virtual (VPN, por sus siglas en inglés) y conectarse a una red segura mientras aparentaban ser un usuario legítimo. Esto sucede cuando los atacantes ya han logrado infiltrarse exitosamente en la red y han comprometido las credenciales del dominio. En algunos casos, incluso comprometen la autenticación de dos factores utilizada para las conexiones VPN seguras. De esta forma, los delincuentes reingresan a la red utilizando la VPN corporativa, disfrazados de usuarios legítimos, y así se dificulta la detección.

El *malware* "*CoreBot*" reciente también reveló la sofisticación del fraude basado en ingeniería social. CoreBot es una forma relativamente nueva de *malware* bancario que utiliza un diseño modular que les permite a los actores de amenazas personalizar el *malware* para diferentes redes de víctimas, así como para instalar características durante una intrusión, según sea necesario. CoreBot puede realizar la inyección de código en el navegador, la captura de formularios y el robo de credenciales. También incluye un componente de ingeniería social para reunir datos personales de las víctimas, información que las instituciones financieras normalmente usan como una forma secundaria de verificación y se puede usar para cometer un nuevo fraude. Esta funcionalidad puede llevar al robo de identidad e incluso a futuros ataques de ingeniería social que facilitan el fraude.

El fraude cibernético se ha expandido cada vez más hasta incluir dispositivos móviles. Investigadores identificaron recientemente una serie de aplicaciones Android Trojan que se dedican a estafar a instituciones de gestión financiera y a proveedores de servicios en todo el mundo. Apodadas "SlemBunk", estas aplicaciones se hacen pasar por aplicaciones comunes y populares y permanecen ocultas después de la instalación inicial. Tienen la capacidad de suplantar y recolectar credenciales bancarias de autenticación que luego se utilizan para robar identidades y cometer fraudes.

En respuesta a la propagación de ataques de fraudes cibernéticos, los bancos están realizando inversiones masivas para lograr estándares más altos de seguridad. El término "defensa adaptativa" se refiere a una estrategia que incluye un círculo holístico de detección, prevención, análisis y respuesta efectiva a las amenazas ante incidentes. Esto se basa en un ciclo continuo de aprendizaje y mejora. Responder a las preguntas "qué tan bueno debe ser usted" y "qué tipo de programa de administración de riesgo cibernético necesita usted" debe formar parte del debate colaborativo entre todos los interesados relevantes en una organización. Existe una gama de posibles actividades de preparación para cada dominio de seguridad. Estos variarán según la organización, pero estas actividades son la base de un enfoque basado en el riesgo para crear una defensa adaptativa. La atención se centra en comprender las capacidades existentes, garantizar que las iniciativas actuales no se dupliquen, e implementar las medidas necesarias para garantizar el dominio a largo plazo.

Una fuerte y flexible defensa ("defensa adaptativa") contra el fraude cibernético debe centrarse en cuatro áreas principales:

1. Detección: La detección incluye la planificación para lograr la evolución de un programa de seguridad para que esté más allá de la "higiene cibernética básica" y así incluir la inteligencia de una variedad de fuentes y para tomar decisiones programáticas basadas en información relevante procesable. La inteligencia de amenazas debe incluir el conocimiento de los grupos de amenazas conocidos, sus métodos de ataque conocidos y los vectores de ataque anticipados. Identificar el origen de un ataque puede ayudarle a una empresa a comprender los objetivos y los motivos de los atacantes y por qué tienen en la mira a la organización. Desde el punto de vista de la defensa adaptativa, esto significa que un programa de seguridad debe evolucionar desde un monitoreo pasivo a una "cacería" activa en busca de evidencia de actores de amenazas. Este enfoque asume la presencia de un atacante que está utilizando técnicas de intrusión desconocidas.

2. Prevención: La prevención incluye actividades que evitan que los fraudes cibernéticos conocidos y desconocidos se conviertan en incidentes de seguridad importantes. Estas actividades incluyen, entre otras cosas, capacidades adicionales de detección heurística basadas en el comportamiento que pueden evitar que un atacante explote una vulnerabilidad desconocida. La prevención incluye una dimensión humana que se centra en minimizar las amenazas y los riesgos relacionados con el comportamiento y las hazañas humanas (como la ingeniería social), así como el aprendizaje y la educación. Algunos de los principales controles de subdominio para la prevención son:

- Gestión de activos (incluido el territorio clave cibernético).
- Actualización/gestión de parches.
- Gestión de vulnerabilidades.
- Exploración de vulnerabilidades y pruebas del sistema.
- Detección y análisis heurístico, aprendizaje automático y análisis de datos.

Teniendo en cuenta que los ataques cibernéticos son inevitables, enfatizar la detección en lugar de la prevención significa promover una seguridad más efectiva. Este enfoque acepta que la organización puede "perder" a nivel táctico y terminar siendo violada, pero la detección y respuesta rápidas evitarán que la infracción lleve a resultados posteriores aún más graves de fraude.

3. Respuesta: La capacidad de mitigar rápidamente la actividad de fraude es la esencia de una defensa adaptativa. La respuesta debe incluir tanto la capacidad para mitigar el daño como la medición del tiempo que es necesario para la mitigación después de un incidente. La respuesta debe incluir los siguientes controles de subdominio:

- Administración de incidentes.
- Gestión de la continuidad del servicio (que tiene una fuerte dependencia de la identificación y gestión de activos).
- Gestión de la dependencia externa.
- Comunicación interna y externa.
- Gestión de las partes interesadas.

La estrategia de respuesta debe establecer, entre otras cosas, un coordinador de respuesta a incidentes y definir protocolos que informen a las partes interesadas clave, de manera eficiente y efectiva. Estos protocolos deben regir los requisitos de revelación de privacidad y la asignación de flujos de trabajo para la investigación, remediación, comunicación y ejecución del plan de respuesta.

4. Análisis: El análisis incluye contención, investigación forense y reconstrucción de la cadena de destrucción. Una estrategia efectiva debe enfatizar la adaptación basada en el análisis de tipos conocidos de fraude cibernético. Este análisis posterior al incidente constituye la base de una respuesta adaptativa al ajustar los controles en función de los riesgos reales conocidos. El análisis de la actividad conocida puede promover la adopción de medidas técnicas y organizativas adecuadas para salvaguardar los datos, sistemas y otros activos en un nivel de seguridad adecuado a los riesgos reales. Esto enfoca los recursos en la prevención, detección y minimización del impacto de metodologías de amenazas conocidas. Comprender las tácticas y los métodos de los atacantes promueve la toma de decisiones informada, la integración (mejorada) de la inteligencia y la respuesta oportuna. El análisis estratégico y táctico también desempeña un papel importante en el pronóstico de tendencias, capacidades e intenciones de los atacantes, mejorando aún más las capacidades antifraude de una organización.

El panorama general del fraude cibernético en América Latina todavía presenta la persistencia de amenazas de fraude cibernético que dominaron otras regiones en el pasado[21]. Las personas individuales siguen siendo el "punto de entrada" preferido para los ataques de fraude[22] en América Latina. El uso de tácticas de suplantación de identidad (*phishing*) e ingeniería social aumenta el número de víctimas disponibles para ser blancos, especialmente en el contexto de las instituciones financieras, donde cada empleado puede ser un elemento clave en el flujo de trabajo de las liberaciones de pagos y de otras operaciones sensibles.

Por último, la aparición de nuevas tecnologías, como los pagos móviles[23], las criptomonedas y las tecnologías financieras ampliadas crea nuevas inquietudes relacionadas con el fraude cibernético, al expandir el panorama de amenazas.

Tendencias en políticas públicas de fraude cibernético en América Latina

América Latina regularmente se ubica entre las regiones con la mayor tasa de incidentes de delitos cibernéticos. Este ranking se debe a varias razones, pero incluye el hecho de que los países latinoamericanos han sido históricamente lentos en mantenerse a buen ritmo en actualización de políticas y estrategias nacionales contra el delito cibernético[24]. Esto se evidencia tanto a nivel nacional[25] como internacional[26]. En este entorno, ha proliferado una gran cantidad de fraudes cibernéticos que comprenden ataques dirigidos contra instituciones financieras (bancos, pasarelas de pago[27]) y ataques que tienen a sus clientes como blanco. Si se considera su lado positivo, los mercados financieros latinoamericanos son tecnológicamente sólidos y sofisticados. Estas plataformas electrónicas avanzadas, si se combinaran con políticas y estándares de seguridad adecuados, podrían mejorar la resiliencia regional a la actividad de fraude cibernético y proporcionar una solución a los desafíos emergentes.

Ante los desafíos, se están produciendo adelantos positivos en América Latina. Como ejemplo, la cooperación entre bancos y agencias internacionales tiene el potencial de perfeccionar los controles e intercambiar información vital sobre amenazas. Un ejemplo reciente es un acuerdo firmado en 2018 entre Interpol y Banco do Brasil. Este fue diseñado para promover la cooperación, y un empleado de Banco do Brasil se trasladó por comisión de servicio al equipo de Interpol en Singapur para poder apoyar el intercambio de información[28]. La colaboración público-privada también puede realizarse a nivel nacional local, como en el caso de un acuerdo entre la Asociación Brasileña de Bancos (Febraban) y la Policía Federal de Brasil, según la cual los representantes de los bancos quedan disponibles para cooperar con los agentes del orden público[29].

Los resultados positivos de estas acciones de colaboración, junto con el progreso en la armonización de las normas de seguridad en los sectores público y privado, han mostrado el camino a seguir para crear un entorno mejorado de ciberseguridad y una estrategia antifraude. Las estrategias integradas de ciberseguridad también se han incluido a los planes nacionales de ciberseguridad, como en el caso de Uruguay[30] y Chile[31]. Estos planes generalmente contemplan las siguientes medidas:

- Nombramiento de un oficial de ciberseguridad independiente de alto nivel en cada agencia.
- Mejora de los reglamentos técnicos sobre ciberseguridad (que también regula la prueba electrónica, la protección de la red y la seguridad de la información).
- Inventario interno, evaluación y plan de acción de ciberseguridad.
- Desarrollo de la política de ciberseguridad.
- Desarrollo de estándares de ciberseguridad.
- Equipo de respuesta de emergencia de seguridad cibernética obligatorio e informe de incidentes.

Dado el papel crítico que desempeñan los mercados financieros en la economía nacional, las autoridades supervisoras locales[32] han creado regulaciones con contenidos similares a los de los planes nacionales de ciberseguridad y los controles de replicación. Esto se evidencia en Brasil[33], donde la política pública exige el cumplimiento no solo de las instituciones financieras, sino también de los proveedores que están integrados en su ecosistema. Sin embargo, la tendencia de construir directrices coherentes y su implementación enfrenta un desafío particular en la región. Existe la necesidad de ofrecer políticas con la escalabilidad necesaria para hacerlas compatibles con el perfil altamente diverso de las instituciones financieras[34], tanto en términos de restricciones geográficas como de tamaño.

Otro asunto que ahora afecta la política pública de seguridad cibernética es el desarrollo de nuevas leyes de privacidad de datos[35]. Dado que la mayoría de los países de América Latina tienen sistemas legales influenciados por modelos europeos, existe una propensión natural hacia la adopción de estándares que sigue la tendencia de la UE a privilegiar la protección de la privacidad sobre la seguridad. Las leyes de seguridad nacional también son otro factor que están afectando las políticas públicas de seguridad cibernética en América Latina. Muchos países ahora están clasificando los mercados financieros como un activo crítico. Todos estos factores de política pública afectan la respuesta de las instituciones financieras para mejorar la seguridad y combatir el fraude en línea.

La armonización de las políticas públicas entre los países latinoamericanos es un tema que requiere mayor atención. La cooperación técnica por medio de programas de desarrollo de capacidades y la cooperación técnica entre los equipos de respuesta a incidentes tiene antecedentes bien establecidos. Sin embargo, el desarrollo de políticas y normas regionales[36] más armonizadas mejoraría la resiliencia de la seguridad cibernética y la prevención del fraude[37]. Esto es especialmente cierto en el entorno del fraude cibernético, donde una estrategia regional coordinada y una respuesta coordinada pueden ser decisivas para el éxito.

La respuesta de las autoridades de seguridad a los fraudes cibernéticos

Los delincuentes cibernéticos han diversificado el enfoque de sus ataques. Inicialmente se concentraban en las plataformas de TI tradicionales, como las computadoras convencionales o portátiles, y ahora han ampliado sus esfuerzos para atacar dispositivos móviles[38]. A pesar de estos desafíos, muchas iniciativas de las autoridades de seguridad para investigar a grupos de delitos cibernéticos han resultado valiosas[39]. Algunas de las últimas tendencias de fraude cibernético en América Latina incluyen la publicidad maliciosa[40] (*malvertising*, o *malware* difundido a través de la publicidad en línea), las explotaciones de Internet de las cosas[41], y los ataques relacionados con las criptomonedas[42]. Los delincuentes cibernéticos activos en la región han diversificado y mejorado sustancialmente su portafolio de técnicas[43] lo que ha significado que esto ahora requiera una atención y una respuesta especial por parte de los agentes del orden público.

En el futuro, algunas proyecciones prevén[44] la propagación geográfica de grupos más pequeños de ciberdelincuentes, que surgirán del desmantelamiento de grupos más grandes. También podrá aumentar el fraude perpetrado mediante la apropiación indebida de datos biométricos (reconocimiento facial y otros). Estas tendencias pueden exacerbar la brecha entre la actividad de delitos cibernéticos y la capacidad de respuesta de las instituciones financieras en la región.

Las dimensiones técnicas y transnacionales del fraude cibernético crean numerosos retos para los organismos encargados de hacer cumplir la ley. Abordar los requisitos transnacionales de investigación requiere cooperación público privada y cooperación legal mutua. La cooperación internacional puede ser formal o informal. En general, los mecanismos formales para la cooperación internacional se desarrollan a través de tratados bilaterales o multilaterales, mientras que las medidas informales son aquellas desarrolladas a través de líneas de comunicación no oficiales con el propósito de compartir información[45].

El principio general para la asistencia legal mutua entre los agentes del orden público se deriva del principio general para la cooperación internacional. Por lo tanto, al igual que la cooperación internacional en general, el Convenio sobre ciberdelincuencia del Consejo de Europa establece que cada Estado debe:

"prestarse asistencia mutua en la mayor medida posible para fines de investigaciones o procedimientos relacionados con delitos penales concernientes a sistemas informáticos y datos, o para la recopilación de pruebas en forma electrónica de un delito penal... adoptar las medidas legislativas y de otra índole que sean necesarias para cumplir las obligaciones... [y] en circunstancias urgentes, realizar solicitudes de asistencia mutua o comunicaciones relacionadas con el mismo por medios rápidos de comunicación".

El mecanismo más formal y tradicional para obtener evidencia de otros países es a través de cartas rogatorias, que son solicitudes emitidas por los tribunales de un Estado requirente a los tribunales del Estado requerido, para que el Estado requerido asista, a través de su poder judicial, en la recopilación de pruebas en el Estado requerido, para una investigación en curso. Sin embargo, los profesionales deben tener en cuenta de que no existe ninguna obligación legal internacional para cumplir con una solicitud en una carta rogatoria.

El segundo mecanismo formal para solicitar asistencia legal internacional es a través de un tratado de asistencia legal mutua (MLAT, por sus siglas en inglés). Los MLAT son marcos y procedimientos convenidos, mediante los cuales los Estados pueden solicitar asistencia legal mutua, como la recopilación de pruebas o la detención de sospechosos de delitos, y pueden ser bilaterales o multilaterales, según el tratado en particular[46]. Desarrollados como una alternativa a las cartas rogatorias, los MLAT han establecido nuevas formas de relaciones de cooperación entre los agentes del orden público de diferentes Estados que simplifican y estandarizan los procedimientos para buscar asistencia legal extranjera. Si bien los MLAT son generalmente mucho más rápidos que las cartas rogatorias, "las investigaciones que requieren asistencia legal mutua en general toman aún más tiempo que las cartas debido a los engorrosos trámites formales, que son demorados, en las comunicaciones entre los agentes del orden público"[47].

Además de los mecanismos formales, existen maneras informales de cooperación, como el intercambio de inteligencia entre diferentes países. La solicitud de asistencia por medio de una comunicación informal implica el contacto directo entre los agentes del orden público y las entidades del sector privado. Las solicitudes de asistencia, generalmente en forma de información, ocurren a nivel de investigación que se desarrollan gracias a unas relaciones de largo alcance. A pesar de la rapidez con que se puede solicitar y cumplir la asistencia con medidas informales de cooperación internacional, estas medidas voluntarias a menudo son limitadas porque las solicitudes como las de las pruebas deben ser autorizadas a través de los canales legales apropiados. Es cada vez más común que los agentes del orden público coloquen enlaces de esas agencias dentro de embajadas o consulados en países extranjeros para facilitar el trámite de las solicitudes de asistencia legal. Ejemplos de tales puntos de contacto cooperativo son las redes G8 y 24/7 del Consejo de Europa que facilitan una amplia gama de gestiones de cooperación internacional tanto para las solicitudes de cooperación formal como informal[48].

Tipos de asistencia legal mutua específica para el delito cibernético

Preservación y revelación rápida de datos informáticos almacenados:

Al reconocer que los datos informáticos son "altamente volátiles" y se pueden eliminar con la sola opresión de una tecla, muchos tratados internacionales que combaten la ciberdelincuencia incluyen disposiciones de procedimiento para la conservación y revelación rápida de los datos informáticos almacenados[49]. Este mecanismo de procedimiento garantiza la disponibilidad de "datos que están pendientes en un proceso,

más largo y más complicado, de ejecución de una solicitud formal de asistencia mutua, que puede llevar semanas o meses"[50].

Para conocer un ejemplo de una de esas disposiciones contenidas en un acuerdo internacional, véase el Artículo 29 del Convenio sobre ciberdelincuencia del Consejo de Europa:

Artículo 29 *Conservación rápida de datos informáticos almacenados.*

> **1.** Una Parte puede solicitarle a otra Parte que ordene u obtenga de otro modo la conservación rápida de los datos almacenados por medio de un sistema informático, que esté ubicado dentro del territorio de esa otra Parte y respecto del cual la Parte solicitante tiene la intención de presentar una solicitud de asistencia mutua para la búsqueda o el acceso similar, la incautación o la seguridad similar, o la revelación de los datos.

Cabe señalar que si bien este procedimiento está diseñado para ser mucho más rápido que la asistencia mutua tradicional, también es menos intrusivo, ya que la parte requerida no tiene que realmente adquirir la posesión de los datos por parte de su custodio[51]. A menudo denominada una "congelación rápida", esta herramienta de investigación tiene la "ventaja de ser rápida y protectora de [privacidad]" porque la información solo se le divulga a un funcionario gubernamental autorizado hasta que se cumplan los criterios de procedimiento para la revelación completa de una solicitud de asistencia mutua[52]. En última instancia, el procedimiento de congelación rápida garantiza que los datos esenciales para las gestiones de investigación de los agentes del orden público no se pierdan irremediablemente[53].

> **2. Preservación rápida y revelación parcial de datos de tráfico**[54].
> No es inusual que se le solicite a un Estado que conserve y/o divulgue los datos de tráfico de una transmisión que ha pasado a través de una computadora ubicada en su territorio para rastrear la transmisión hasta su origen e identificar al autor del delito, o para conseguir pruebas[55].

Artículo 30 *Revelación rápida de datos de tráfico conservados*

> **5.** Cuando, en el curso de la ejecución de una solicitud [para la preservación y revelación de datos informáticos] para preservar los datos de tráfico relacionados con una comunicación específica, la Parte requerida descubra que un proveedor de servicios en otro Estado estuvo involucrado en la transmisión de la comunicación, la Parte requerida deberá revelarle rápidamente a la Parte solicitante una cantidad suficiente de datos de tráfico para identificar al proveedor del servicio y la ruta a través de la cual se transmitió la comunicación.
>
> **6. La revelación de datos de tráfico según el párrafo 1 solo podrá ser denegada si:**
>
> (a) la solicitud se refiere a un delito que la Parte requerida considera un delito político o un delito relacionado con un delito político; o
> (b) la Parte requerida considera que la ejecución de la solicitud puede perjudicar su soberanía, seguridad, orden público u otros intereses esenciales.

La revelación de datos de tráfico conservados les brinda a las autoridades de investigación la capacidad de entregarles a los Estados, que han solicitado el procedimiento de "congelación rápida" que se detalla más arriba, información adicional sobre la identidad de un proveedor de servicios y la ruta de la comunicación utilizada para cometer su delito[56].

7. **Órdenes de presentación**

Una orden de presentación les permite a los agentes del orden público obligar a una persona o proveedor de servicios en su territorio a entregar datos informáticos almacenados o información del suscriptor[57]. También les provee a las autoridades un mecanismo de aplicación más flexible en los casos en que se necesite la revelación de datos informáticos, y ayuda a que los proveedores de servicios se sientan más cómodos con dichas divulgaciones al proporcionarles una base legal para suministrar esa información[58].

Artículo 18 *Orden de presentación*[59]

1. Cada Parte adoptará las medidas legislativas y de otra índole que sean necesarias para facultar a sus autoridades competentes para ordenarle:

(a) a una persona en su territorio que envíe datos informáticos específicos que se encuentren en posesión o control de esa persona, que estén almacenados en un sistema informático o en un medio de almacenamiento de datos informáticos; y
(b) a un proveedor de servicios que ofrece sus servicios en el territorio de la Parte que envíe información de suscriptores relacionada con dichos servicios en posesión o control de dicho proveedor de servicios.

La información del suscriptor, de acuerdo con la disposición anterior, se define como "cualquier información tenida en forma de datos informáticos o cualquier otra forma en poder de un proveedor de servicios, relacionada con los suscriptores de sus servicios" que pueda establecer "el tipo de servicio de comunicación utilizado", "la identidad del suscriptor" o "dirección geográfica", así como "cualquier otra información... disponible sobre la base del arreglo o acuerdo de servicio"[60]. Esta información a menudo es necesaria para determinar los servicios técnicos que se utilizaron para cometer un delito informático y para ayudarles a los agentes del orden público a identificar con precisión a la persona que presuntamente cometió estos delitos[61].

4. **Asistencia mutua para la obtención en tiempo real de datos relativos al tráfico.**

Esta herramienta de investigación les brinda a los agentes del orden público la capacidad de adquirir "la obtención en tiempo real de datos relativos al tráfico y la intercepción en tiempo real de los datos de contenido asociados con comunicaciones específicas transmitidas por un sistema informático" tanto de "autoridades competentes" como de "proveedores de servicios"[62]. "El Convenio sobre ciberdelincuencia ilustra este mecanismo procesal en un instrumento internacional.

Artículo 33 *Asistencia mutua para la obtención en tiempo real de datos relativos al tráfico*[63].

1. Las Partes se prestarán asistencia mutua en la obtención en tiempo real de datos relativos al tráfico asociados con comunicaciones específicas en su territorio transmitidos por medio de un sistema informático. Con sujeción a lo dispuesto en el párrafo 2, esta asistencia se regirá por las condiciones y procedimientos previstos en la legislación nacional.

2. Cada Parte proporcionará dicha asistencia al menos con respecto a los delitos para los cuales la obtención en tiempo real de datos relativos al tráfico estaría disponible en un caso nacional similar.

Contar con un mecanismo que pueda ser empleado por los agentes del orden público para obtener la recopilación de datos en tiempo real es esencial para llevar a los infractores ante la justicia, ya que cierta información como los datos de tráfico ya no estará disponible una vez que el autor de la intrusión cese su actividad o cambie su ruta de acceso[64].

5. **Asistencia mutua en relación con la interceptación de datos relativos al contenido.**
La interceptación de datos relativos al contenido implica el uso de medios técnicos para recopilar o registrar "datos de contenido, en tiempo real, de comunicaciones específicas (...) transmitidas por medio de un sistema informático"[65]. Los datos de contenido difieren de otras formas de información en el computador, como son los datos de tráfico, porque en lugar de entregar información sobre el remitente y el destinatario previsto de una comunicación, las autoridades tienen conocimiento de la comunicación de información real, o sea, el contenido de la transmisión[66]. Se ilustra una disposición, con respecto a la intercepción, en El Convenio de Budapest sobre la ciberdelincuencia que establece:

Artículo 34 *Asistencia mutua en relación con la interceptación de datos relativos al contenido*

Las Partes se prestarán asistencia mutua en la recopilación o el registro en tiempo real de datos de contenido de comunicaciones específicas transmitidas por medio de un sistema informático en la medida en que lo permitan sus tratados y las leyes nacionales aplicables[67].

Esta herramienta de investigación, que actualmente es un área emergente de asistencia mutua, es muy útil para determinar si una comunicación es de naturaleza ilegal o para recopilar pruebas de delitos pasados o futuros[68]. Sin embargo, debido a que esta forma de intercepción es intrusiva, se han privilegiado las leyes nacionales y los tratados aplicables con respecto a cómo dichos procedimientos deben ser llevados a cabo por los agentes del orden público[69].

6. **Retención de datos.**
La retención de datos obliga a los proveedores de servicios a guardar datos de tráfico durante períodos de tiempo específicos y es un intento de evitar la eliminación automática de ciertos tipos de datos que pueden ser cruciales para una investigación penal[70]. La retención de datos generalmente no es una obligación establecida a nivel internacional, a pesar del hecho de que puede tener serias consecuencias sobre la efectividad de una investigación internacional de delitos cibernéticos.

7. **Órdenes de revelar claves de cifrado.**
La tecnología de cifrado crea serias dificultades para los agentes del orden público. Por ejemplo, incluso si los investigadores son lo suficientemente afortunados como para haber actuado con rapidez y recuperado los datos de contenido que puedan ayudar a detener a un delincuente cibernético, es posible que los agentes del orden público no puedan ver los datos obtenidos si el autor los había cifrado previamente. Para evitar este grave impedimento para el éxito de la investigación, los agentes del orden público tienen la capacidad de asegurar una orden de presentación, que se puede utilizar para forzar a quien tenga la clave del cifrado que se la entregue.

8. **Puntos de contacto 24/7**
Para facilitar la asistencia legal mutua en las investigaciones de delitos cibernéticos, muchos instrumentos obligan a los Estados a establecer "Puntos de contacto 24/7" que están disponibles las veinticuatro (24) horas al día, siete (7) días a la semana para gestionar las solicitudes de asistencia en caso de que surjan. Por ejemplo:

Artículo 35 *Red 24/7*

2. (a) El punto de contacto de una Parte tendrá la capacidad de llevar a cabo comunicaciones con el punto de contacto de otra Parte rápidamente.

(b) Si el punto de contacto designado por una Parte no forma parte de la autoridad o autoridades responsables de la asistencia mutua internacional o de extradición, el punto de contacto se asegurará de que pueda coordinar con dicha autoridad o autoridades rápidamente.

3. Cada Parte garantizará que haya personal capacitado y equipado disponible para facilitar la operación de la red.

La "tarea crítica" que deben realizar las Redes 24/7 es la facilitación inmediata de las solicitudes de asistencia mutua, ya sea por sí mismas o por medio de las autoridades competentes ubicadas dentro de la comunidad de aplicación de la ley. Concomitante con la obligación es el requisito de que cada estado garantice que sus redes 24/7 tengan tanto la experiencia como los recursos para cumplir su mandato.

5. Cada Parte designará un punto de contacto que esté disponible las veinticuatro horas, los siete días de la semana, para garantizar la prestación de asistencia inmediata para efectos de investigaciones o procesos relacionados con delitos penales referentes a sistemas informáticos y datos, o para la recopilación de pruebas de un delito penal en forma electrónica. Dicha asistencia incluirá la facilitación o, si lo permite su legislación y prácticas nacionales, la implementación directa de las siguientes medidas:

a) la prestación de asesoramiento técnico;
b) la conservación de datos de conformidad con los artículos 29 y 30;
c) la recopilación de pruebas, el suministro de información legal y la localización de sospechosos.

A. Instrumentos cooperativos internacionales

Hay tres formas en que los agentes del orden público pueden invocar un instrumento para la cooperación internacional. Primero, los procedimientos pertinentes pueden formar parte de acuerdos multilaterales internacionales, como la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional (UNTOC[71], *por sus siglas en inglés*), o convenciones regionales, como la Convención Interamericana sobre Asistencia Mutua en Materia Penal[72], la Convención Europea de Asistencia Mutua en Materia Penal[73] o el Convenio sobre la ciberdelincuencia del Consejo de Europa[74].

Segundo, el procedimiento cooperativo internacional puede establecerse a través de acuerdos bilaterales. En general, dichos acuerdos se refieren a solicitudes específicas que pueden presentarse y definen los procedimientos y formas de contacto pertinentes, así como los derechos y obligaciones de los Estados requirentes y requeridos[75]. Por ejemplo, Australia ha firmado más de 30 acuerdos bilaterales con otros países que regulan aspectos de la extradición[76]. Aunque se menciona en algunos acuerdos bilaterales, es incierto hasta qué punto los acuerdos existentes regulan adecuadamente el delito cibernético[77].

Si no es aplicable un acuerdo multilateral ni bilateral, la cooperación internacional generalmente debe basarse en la cortesía internacional, basada en la reciprocidad[78]. La cooperación basada en acuerdos bilaterales y la cortesía depende en gran medida de las circunstancias del caso real, la naturaleza del tratado bilateral, si lo hubiere, y los países involucrados.

Resumen de los instrumentos de cooperación relevantes

Muchos de los instrumentos relevantes para la cooperación internacional en la lucha contra el delito cibernético cubren áreas sustantivas similares, como la criminalización, la seguridad cibernética y el comercio electrónico. Sin embargo, las disposiciones más relevantes para fines de cooperación internacional son aquellas que abordan la jurisdicción, la cooperación internacional en las formas de asistencia legal mutua y la extradición, y otras formas específicas de cooperación internacional directamente relacionadas con el delito cibernético. Ejemplos son la conservación expedita de información por computadora o las órdenes de presentación. A continuación se estudiarán estas disposiciones pertinentes en varios instrumentos importantes.

1. El Consejo de Europa (COE) - Convenio sobre la ciberdelincuencia (2001)

El Convenio de Budapest es un instrumento relacionado con el delito cibernético que fue redactado en 2001 por el Consejo de Europa. El alcance de las disposiciones de cooperación internacional en la Convención incluye todos los delitos que se pueden clasificar como "delitos cibernéticos"[79]. Redactado para "lograr una mayor unidad" entre el Consejo de Europa y otros signatarios estatales, la Convención espera crear "una política penal común dirigida la protección de la sociedad contra el delito cibernético, entre otras cosas, mediante la adopción de una legislación apropiada y el fomento de la cooperación internacional"[80].

El artículo 23 del Convenio de Budapest contiene tres principios generales relativos a la cooperación internacional en la investigación del delito cibernético. Primero, se prevé que los miembros brinden cooperación en las investigaciones internacionales en la mayor medida posible, lo que refleja la importancia de la cooperación en las investigaciones internacionales sobre delitos cibernéticos[81].

En segundo lugar, el Artículo 23 establece que la cooperación "en la mayor medida posible" se aplica no solo a los "delitos relacionados con los sistemas informáticos y datos", sino también "para la recopilación de pruebas en formato electrónico" para cualquier otro delito penal[82]. Por lo tanto, la cooperación, en la medida de lo posible, en el marco de la Convención, debería realizarse en las investigaciones de delitos cibernéticos, así como en las investigaciones penales tradicionales en las que puede haber prueba electrónica[83]. El tercer principio establecido en el artículo 23 es que las disposiciones de la Convención que se ocupan de la cooperación internacional no sustituyen, sino que complementan, otras disposiciones de los acuerdos internacionales relativos a la asistencia judicial recíproca y la extradición o disposiciones pertinentes de derecho interno relativas a la cooperación internacional[84]. La intención de los redactores de El Convenio de Budapest no era crear un régimen independiente de asistencia legal mutua, sino establecer una base legal para llevar a cabo la cooperación internacional en caso de que no existiera ninguna entre las partes afectadas por los delitos cibernéticos[85].

Con respecto a la asistencia mutua, el párrafo 1 del Artículo 25 complementa los principios establecidos en el Artículo 23 en el sentido de que establece que las partes se prestarán asistencia "en la medida de lo posible"[86]. Además, el párrafo 3 contiene una de las disposiciones más importantes del Artículo 25, es decir, la creación de una base para la comunicación urgente entre las partes en las investigaciones de delitos cibernéticos, siempre que dicha comunicación se realice con los "niveles adecuados de seguridad y autenticación"[87]. Una serie de investigaciones de delitos cibernéticos a nivel nacional fracasan porque son muy demorados y se eliminan datos importantes antes de que se tomen las medidas procedimentales para preservarlos. Consecuentemente, el Convenio prevé un medio de comunicación rápido con la esperanza de que esas autoridades[88] puedan disponer de más pruebas/datos necesarios para las investigaciones transfronterizas.

Además del Convenio de Budapest, otros instrumentos globales de asistencia mutua incluyen la Comunidad Económica de los Estados de África Occidental (CEDEAO) en su Directiva sobre la lucha contra el delito cibernético dentro de la CEDEAO (2009), la Organización de Cooperación de Shangai (OCS) en su Acuerdo sobre Cooperación en el Campo de Seguridad de la Información Internacional (2010), la Unión Africana (UA) en su Proyecto de Convención sobre el Establecimiento de un Marco Legal Propicio para la Ciberseguridad en África (2012), la Liga de los Estados Árabes (LEA) en su Convención Árabe para Combatir los Delitos de Tecnología de la Información (2012). Muchas de las disposiciones en estos mecanismos de cooperación son similares a las del Convenio sobre delito cibernético del Consejo de Europa anterior[89].

Conclusiones y resumen

Es fundamental enfatizar que aunque el fraude cibernético puede estar más avanzado que el fraude tradicional, el objetivo de los delincuentes sigue siendo el mismo: robar información o dinero lo más rápidamente posible. El ciberespacio solo crea mayores desafíos para combatir delitos viejos. También es crítico enfatizar los beneficios de la tecnología. Las computadoras no cometen delitos, las personas cometen delitos. La buena tecnología está siendo abusada para cometer fraude. Es importante que los encargados de la formulación de políticas y del orden público reconozcan que el actor de la amenaza es una persona y no una máquina.

Sin embargo, la amenaza del fraude cibernético requiere un enfoque continuo en la capacitación, políticas efectivas, desarrollo de capacidades y cooperación. La respuesta del sector financiero está mejorando, aunque sigue existiendo una brecha entre la conciencia y los recursos gastados para combatir la amenaza del fraude cibernético. El objetivo debe ser mejorar el intercambio de inteligencia de los indicadores de fraude, mejorar las plataformas de cooperación público-privada y entregarle al cliente una experiencia bancaria que sea segura y normal. Los ataques cibernéticos y el fraude cibernético representan una amenaza importante para la seguridad y estabilidad global de los mercados financieros críticos. Estas empresas son la base económica de todas las economías. Invertir en recursos y capacidades para combatir esta amenaza es una inversión en la seguridad y el futuro de América Latina.

Riesgo cibernético y su relación con el sistema financiero en América Latina

José Marangunich

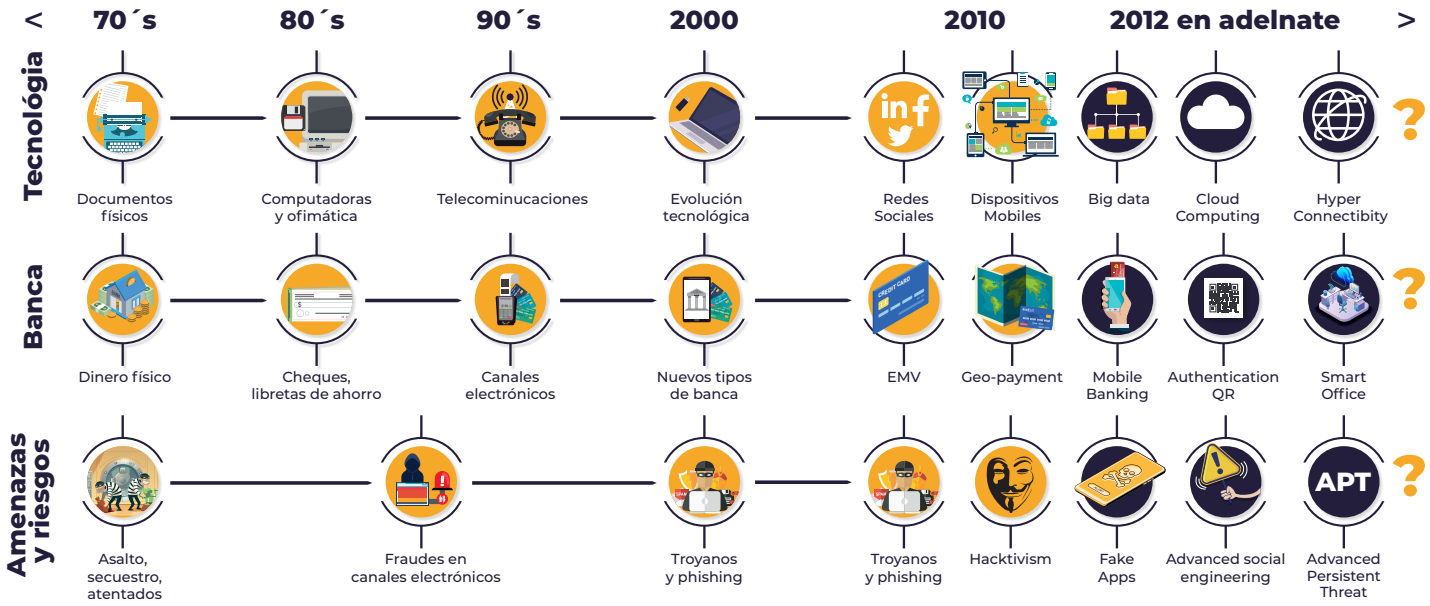
A. Contexto de la transformación del sistema financiero en el siglo XXI

Cuando hacemos mención al proceso de transformación que viene enfrentando el sistema financiero a nivel global en el presente siglo, encontramos definiciones tan complejas como el inicio de una nueva revolución industrial, la transformación de las empresas de tecnología y bancos migrando a ser empresas de software, entre otras tantas definiciones. Todas hacen mención o están orientadas a fijar un cambio radical en la definición de los planes, propósitos y enfoques que las entidades financieras usualmente tienen como norte.

Actualmente, los propósitos de las entidades financieras tienen como principales razones de ser el servicio a sus clientes, el refuerzo de sus vínculos con las partes interesadas y la responsabilidad social empresarial. De igual manera, les es importante adecuar los modelos de negocio a la modernidad, lo cual conlleva a lograr esquemas de eficiencia con satisfacción en la experiencia del usuario, mejorar su comunicación con un cliente más informado y poner a disposición una diversidad de opciones de conexión entre el cliente y la institución; aspectos que han sido recientemente implementados.

Ante este contexto, surgen diversos interrogantes sobre ¿cómo se inició esta transformación?, ¿qué antecedentes tiene?, ¿qué etapas han transcurrido? y ¿qué otros elementos acompañan el proceso de transformación en la industria financiera? A manera de ejemplo, en el Gráfico 1 se presenta una línea de tiempo sobre los cambios en la banca, tecnologías y riesgos que nos puede dar mayores luces sobre lo acontecido en las últimas décadas.

Gráfico 1: Evolución de los riesgos de seguridad en la industria bancaria



Fuente: *Elaboración propia*

La secuencia de cambios disruptivos en la forma de hacer negocios y la interacción con los usuarios de las entidades financieras dan la razón a las singulares definiciones sobre este proceso, en donde podría una entidad planificar su transformación, al punto de ser identificada como empresa generadora de software más que como institución financiera tradicional.

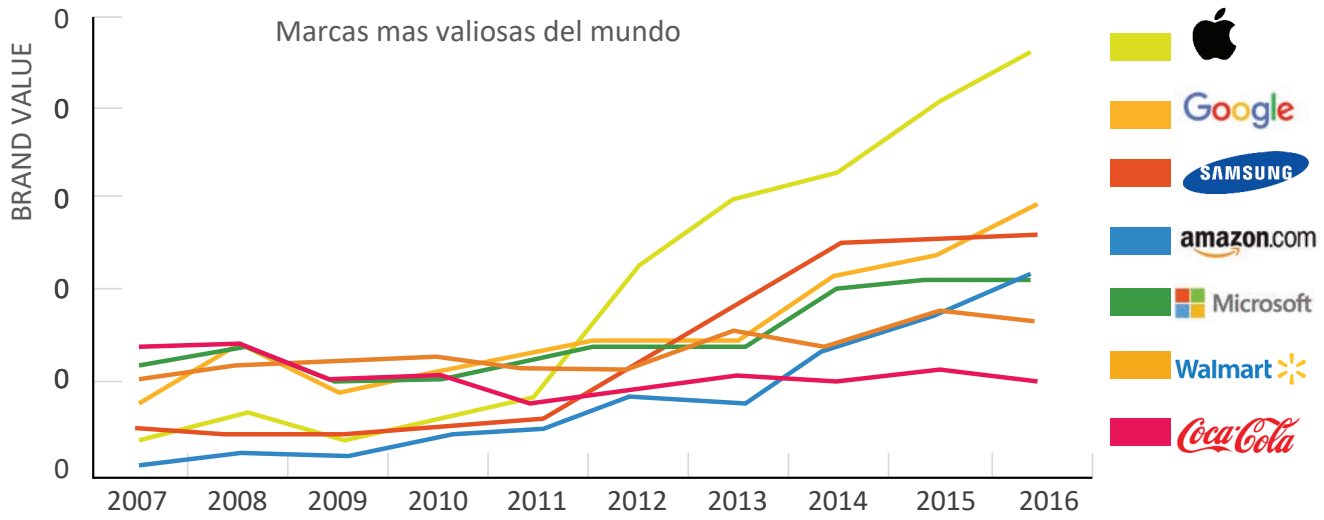
Afinando la visión

Es importante recordar la teoría del ¿por qué? y la presencia de importantes empresas consultoras que con muy buen criterio orientan a las instituciones financieras en el proceso de observar qué ocurría en el contexto, respecto a una modernidad acelerada en la manera de hacer negocios, destacando que los activos más importantes por custodiar en los usuarios son su tiempo y su experiencia de servicio.

Es entonces cuando rápidamente se entiende que no solo se debería continuar viendo qué hacían los bancos en una dinámica muy tradicional, sino más bien, qué otros actores ya estaban en el medio o qué otras industrias venían fijando las reglas de juego sobre el nivel de servicio que debería recibir un usuario/cliente. Además, se debería reconocer que los usuarios en el ecosistema digital venían siendo constantemente informados sobre las propuestas diferenciadas en calidad y medios de interacción que exigían como condición de servicio.

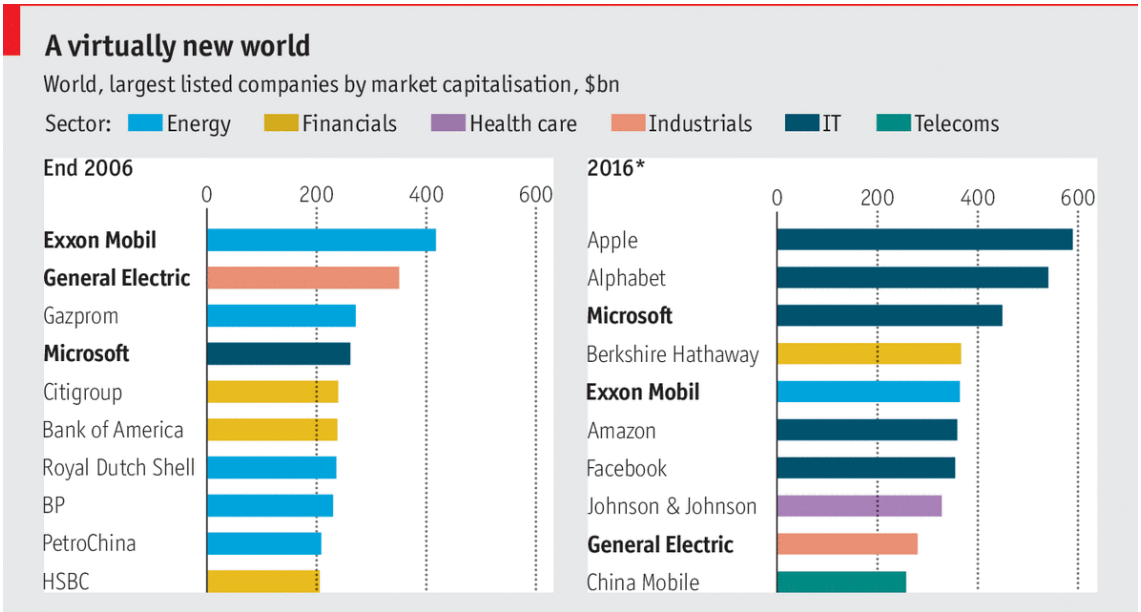
Es así que se identifican a las empresas líderes en tecnología, comunicaciones y servicios como los actores que cambiaron el escenario de la preferencia. Esto se puede apreciar con mucha claridad en los siguientes Gráficos sobre las 10 compañías top en la actualidad, donde ya no están registradas importantes entidades financieras, como sí lo estaban a finales de los años 90 y comienzo del segundo milenio. Sin duda la tecnología marcó la pauta y fijó cuál era el estándar en el mercado (ver Gráficos 2 y 3).

Gráfico 2: Valor de la era digital *(Digital era value)*



Fuente: *Elaboración propia*

Gráfico 3: Un nuevo mundo digital



Fuente: *Blomering, Economist.com*

Cuando compites con todos

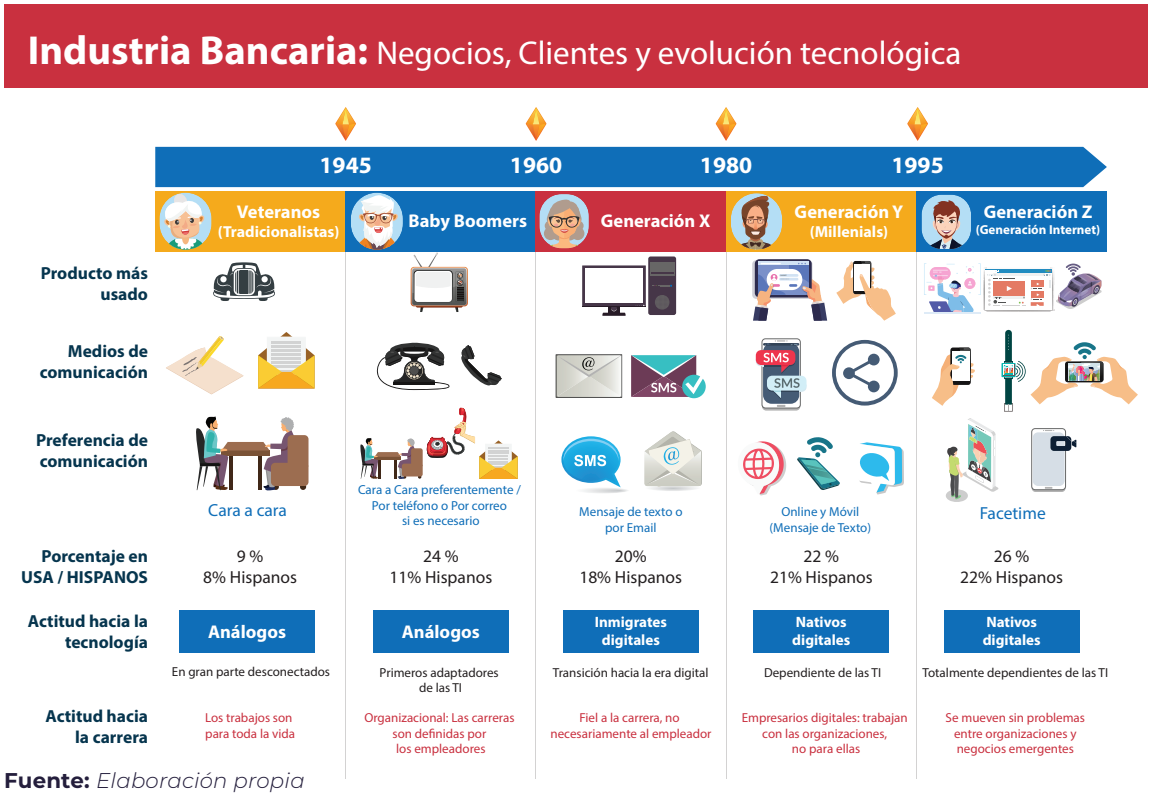
En contexto con lo mencionado en el punto anterior, donde se evidencia la acelerada evolución que generan las organizaciones a través del uso de tecnologías enfocadas al cliente y la aparición de nuevos actores que fijan las reglas de negocio, se adiciona que actualmente las empresas ya no solo ofrecen el producto y/o servicio del rubro donde se posicionan sino también orientan sus estrategias comerciales a ofrecerle al cliente un abanico de opciones para que este pueda adquirir un producto o servicio de manera directa, ágil, flexible y sin intermediaciones, lo cual impulsa y obliga al sistema financiero a generar alternativas de negocio que brinden opciones más accesibles.

Es así como la industria financiera ya no cuenta con competidores fijos en rubros de mercado específicos. Se generan entonces, competencias mixtas donde cualquier empresa puede hacer frente a otra sin ofrecer necesariamente el mismo producto y/o servicio. Asimismo, las empresas digitales crecen aceleradamente con propuestas disruptivas que los clientes valoran y reconocen, generando un caos en el ecosistema tradicional.

La metamorfosis

Las nuevas tecnologías, las diversas alternativas de negocios y sobre todo el centralizar al cliente como el eje de los objetivos de las organizaciones, ha ido evolucionando de generación en generación. Viéndolo como línea de tiempo en el Gráfico 4 se inicia con un alto impacto en la generación X que fue clasificada como "inmigrante digital" y cuyos integrantes incorporaron en sus rutinas nuevos sistemas de comunicación a través del uso de mensajes de textos o correos electrónicos, convirtiéndose así en punto crucial hacia la transición a la era digital.

Gráfico 4: Impacto del cambio generacional



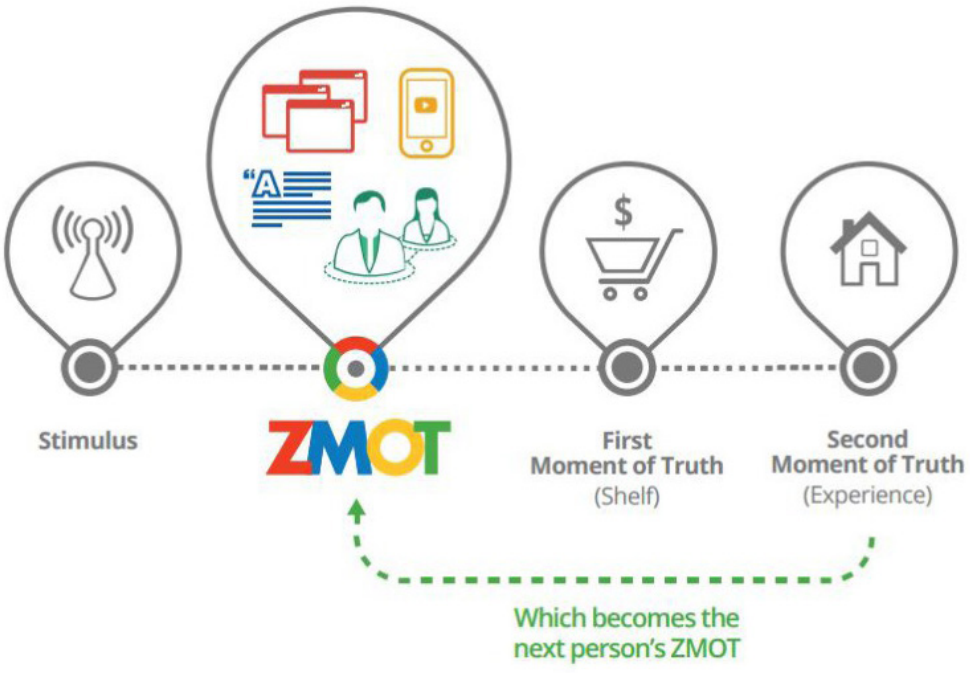
Fuente: *Elaboración propia*

Las siguientes generaciones, los millenials y la generación Z, nacen y crecen siendo nativos digitales, dependientes de las tecnologías de información (TI) y quienes, para desarrollar actividades, tienen la necesidad de estar siempre informados. En este contexto, la interacción con la tecnología es básica y propia de su rutina diaria. Asimismo, generan nuevas ideas y conceptos para el desarrollo de los negocios, siendo ellos quienes direccionan hacia dónde las empresas deben enfocar sus esfuerzos.

Ante esta realidad debemos insistir en que el cliente es la variable fundamental para desarrollar cualquier tipo de estrategia comercial. Por ello, es fundamental que el sistema financiero centralice al cliente como el eje de toda decisión. De lograr entender las preferencias, gustos y necesidades de los clientes, las organizaciones podrán generar diversidad de opciones donde el consumidor sea el que decida y priorice.

Los conceptos antes mencionados hacen que todo cambie. El cliente ya no solo compra un producto directamente en una tienda, sino que a través de las tecnologías recibe el soporte para informarse, incorporando un filtro previo a la toma de sus decisiones, lo que en el marketing moderno se conoce como momento cero de la verdad (Zero Moment of Truth o ZMOT, por sus siglas en inglés). Ver Gráfico 5. Este punto es de vital importancia ya que el cliente tiene un panorama integral del producto o servicio previo a la adquisición y la decisión de compra dependerá de la estrategia comercial y las alternativas de negocio que se le ofrezca. Es por ello por lo que las empresas deben tener este "*driver*" muy en cuenta para su planificación a fin de que identifiquen todos los frentes de acción que tiene el cliente en su proceso de decisión de adquirir un producto y/o servicio, haciendo que la experiencia compartida pueda ser una fortaleza en la captación de clientes y posicionamiento en el mercado.

Gráfico 5: Nuevo modelo mental de marketing *(New mental model of marketing)*



La necesidad del cambio es la metamorfosis que hoy las organizaciones necesitan considerar como parte de la transformación de los modelos de negocios donde se deben incluir los conceptos anteriormente mencionados y los nuevos sistemas de trabajo, metodologías, regulaciones, amenazas, gestión del riesgo y agilidad, entre otros puntos que iremos profundizando en el desarrollo del presente capítulo.

Fuente: *Google*

De lo perfecto a lo necesario

Luego de entender la urgente necesidad del cambio en el sistema financiero que hemos denominado metamorfosis, se plantea el cuestionamiento sobre la factibilidad y sostenibilidad de lograr esa velocidad de cambio con las prácticas y procedimientos que usualmente se vienen aplicando. Es aquí donde las organizaciones deben recurrir a alternativas como consultorías especializadas que generalmente recomiendan operar bajo metodologías ágiles y por fases, generando productos de valor mínimo o MVPs (Minimum Value Products, por sus siglas en inglés). Esto cambia el esquema y estructuras de las organizaciones, logrando formar equipos de alta competitividad con proyectos ejecutables en el corto plazo y con una rendición de cuentas muy bien definido.

El MVP permitió incorporar el concepto de ir cambiando la experiencia digital de esta transformación con entregables de inmediata ejecución en períodos cortos, lo cual permite, entre otras cosas, ser más eficiente en el manejo de los costos al diseñar bajo un patrón de bajo costo y adicionalmente poder rectificar condiciones propias del producto y/o servicio que incluyan elementos complementarios que mejoren la satisfacción del cliente.

Como parte del proceso de transformación digital, esta velocidad trae a discusión lo que se denomina la disyuntiva entre lo necesario y lo perfecto, que se refleja adicionalmente el gran reto de cómo acompañar estos desarrollos desde el lado de la seguridad, considerando que la metodología ágil no necesariamente permite aplicar desde un inicio todas las capas de control o de detección que protejan al servicio y/o producto ante las nuevas amenazas propias de la transformación. Más adelante, en el capítulo de los riesgos, desarrollaremos esta materia con mayor amplitud. Sin embargo, es oportuno referir que este escenario, si bien ha mejorado la manera de hacer el negocio, está siendo bien aprovechado por terceros, quienes por diferentes acciones ponen en condición de riesgo, contingencia o indefensión a una entidad que pueda presentar brechas o vulnerabilidades en sus capas de seguridad.

En resumen y con lo expuesto podemos avizorar que la modernidad de los siglos XXI y siguientes presentará retos en diversos frentes, siendo uno de los más relevantes, el relacionado con las medidas en el ámbito de la ciberseguridad, donde las entidades financieras tendrán una especial demanda tanto a nivel de estrategia, infraestructura, procedimientos y principalmente talento.

En busca del océano azul

Como señalaron W. Chan Kim y Renée Mauborgne, las empresas, incluidas las entidades financieras, alcanzarán el éxito tan esperado en la gestión si, y solo si, el enfoque del modelo de negocio está orientado a la generación de valor vía la innovación, buscando el mejor servicio y la mejor calidad de productos con el consecuente beneficio para quienes los usan o reciben. Estas reglas de juego no siempre son de fácil ejecución debido a la abundancia de océanos rojos (mercados altamente competitivos sin posibilidad de innovación) entre los cual podemos incluir al riesgo de ciberseguridad, el cual a la larga permitirá lograr mejores prácticas en los modelos de negocio, encaminando a lo que se conoce en la industria del negocio, como el esperado océano azul.

Lo antes expuesto de manera muy general y abstracta conlleva a que el propósito, políticas, estrategias, planes de acción y gestión en general incorporen dentro de su propuesta de valor el concepto de seguridad. En ese aspecto las entidades financieras sin duda liderarán en el corto plazo por regulación o por autorregulación y de manera global estas prácticas de gestión. Es importante considerar que estas entidades ya no son una industria cerrada que compite entre sí; hoy el ámbito o alcance de servicios

similares incorpora distintos tipos de industrias, que de una u otra forma, se sitúan en servicios de intermediación, administración de datos o facilitación de servicios de inversión (*fintechs*). Estas empresas mantienen altos índices de satisfacción al cliente, como las empresas de tecnología que son las que van marcando el nivel de avance y la hoja de ruta a seguir.

¿Conocemos con certeza la hoja de ruta a seguir? Ese es interrogante que se escucha hoy en diferentes foros académicos y técnicos; el mensaje a los altos directivos sobre la necesidad de indagar acerca de cómo gestionar la incertidumbre frente al cambio y la transformación.

El presente estudio busca analizar la relación del riesgo cibernético con los sistemas financieros, especialmente en Latinoamérica. Si bien es cierto que el riesgo cibernético tiene actualmente mecanismos, pautas, técnicas, procedimientos, teorías y recursos para ser gestionado, todo se refiere a lo que ocurre y tenemos hoy, lo cual se sabe que no será estático. Como parte de la gestión de la incertidumbre y el proceso de transformación, los riesgos de seguridad se basan de manera relevante en la participación y deberíamos estar muy atentos a este proceso de evolución; en especial si lo que buscamos es llegar a un ambiente parecido al ya mencionado océano azul.

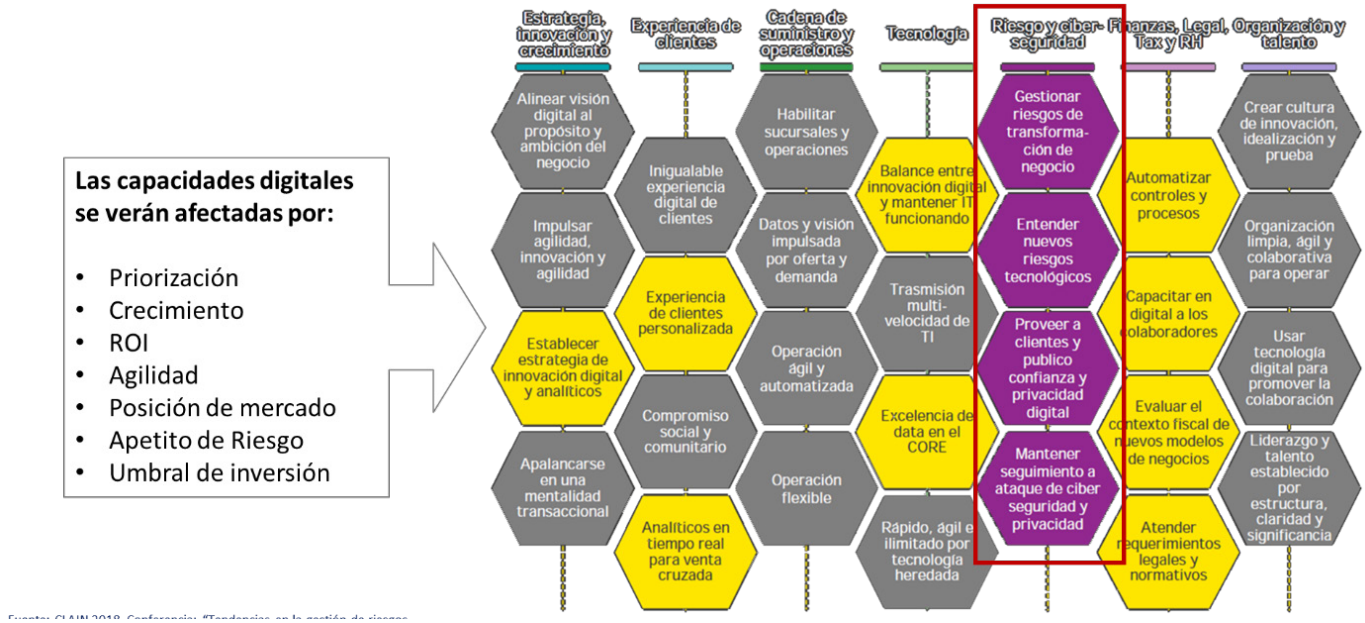
Ciertamente, en el ámbito de la ciberseguridad, continuarán existiendo vulnerabilidades dada las condiciones adversas al desarrollo, al citar escenarios de ciberamenazas, ciberataques, ciberfraude, ciberguerras, entre otros. Latinoamérica resalta como una de las regiones con mayor atención en este reto por estar conformada por países en proceso de desarrollo y con potencial de negocio; además de que actualmente presenta incidencias no menores respecto a las amenazas cibernéticas. En el capítulo siguiente veremos qué se necesita para hacer frente a estos retos.

La gran lista ¿Qué necesito?

Es complejo conocer cuál es la lista exhaustiva con la que se requiere contar para tener en cuenta todos los eventos futuros de incertidumbre. Lo cierto es que hoy tenemos riesgos cibernéticos que necesitamos mitigar. La lista deberá incluir lecciones aprendidas que nos remiten distintas entidades especialistas en ciberseguridad: i) el Marco de Ciberseguridad de NIST (NIST Cybersecurity Framework) en sus diferentes etapas de protección, detección, respuesta, recuperación e identificación; ii) el Comité de Organizaciones Patrocinadoras de la Comisión Treadway - COSO; iii) la ISO 27001; y iv) el COBIT 5 entre otras. En primer lugar, es importante tener en cuenta que el correcto proceso de gestión de este tipo de riesgo debe incluir las etapas de identificación, análisis - medición, evaluación y tratamiento.

En el estudio desarrollado por Ernst & Young (ver Gráfico 6) se mencionan 7 criterios que incluyen: i) la estrategia, la innovación y crecimiento; ii) la experiencia de clientes; iii) la cadena de suministro y operaciones; iv) la tecnología; v) los riesgos y la ciberseguridad; vi) las finanzas; y vii) la organización y talento. Dentro de estos siete, debemos priorizar criterios como la estrategia de la innovación digital, las analíticas en tiempo real, la estabilidad operativa, la gestión de riesgos de transformación de negocios, el monitoreo, la automatización de controles, las capacidades propias y tercerizadas, la retención de talento, el apetito de riesgo, el umbral de inversión y la proyección de crecimiento.

Gráfico 6: Tendencias en la gestión de riesgos en la era digital



Fuente: *CLAIN 2018, Conferencia: "Tendencias den la gestión de riesgos en la era digital"*

B. Transformación, cibernética y riesgos

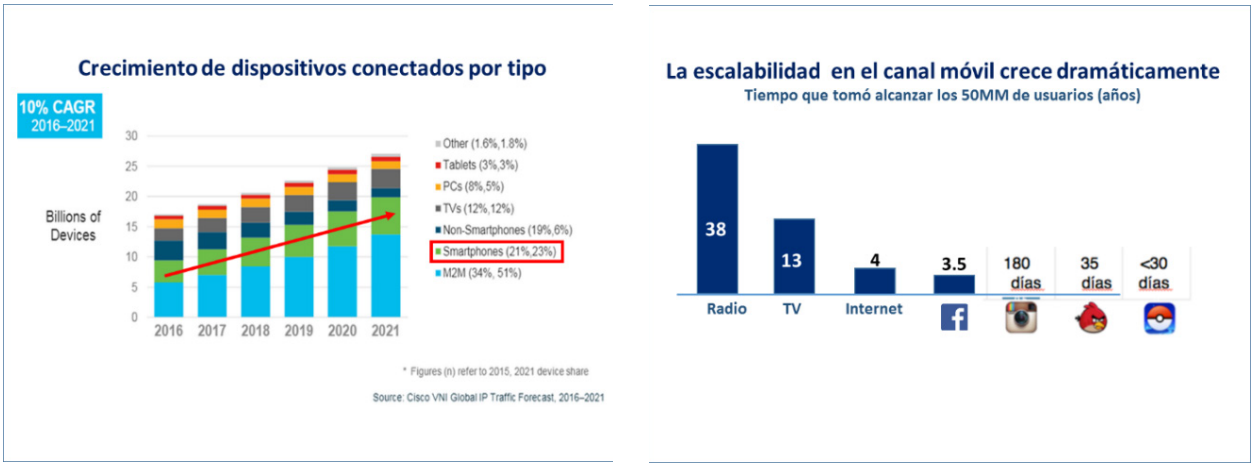
La era digital

La tecnología ha permitido la generación de cambios disruptivos en la forma en que los clientes interactúan con las instituciones financieras (ver Gráfico 7). El nivel de conectividad de los usuarios avanza a pasos acelerados; en los próximos años se proyecta un crecimiento importante en los dispositivos conectados (ver Gráfico 8). El canal digital permite que las empresas estén mucho más cerca de los usuarios generando la posibilidad de alcanzar un mayor número de clientes en menor tiempo.

Gráfico 7: Tecnologías disruptivas en la era digital

Fuente: *ICEMD, Las tecnologías más relevantes y disruptivas de la tecnología digital, 2017*

Gráfico 8: Tecnologías disruptivas en la era digital

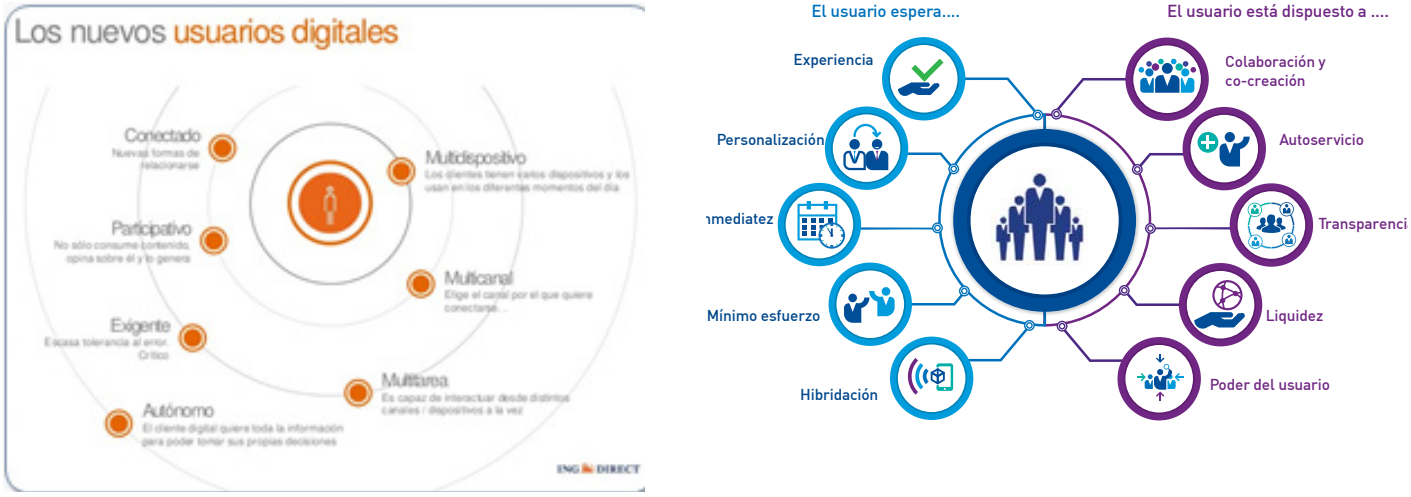


Fuente: *Cisco*

¿Cómo lo hacen? A través del internet de las cosas (IoT, por sus siglas en inglés), los dispositivos físicos y objetos conectados a Internet y entre sí pueden tomar decisiones inteligentes. Asimismo, el internet de todo (IoE, por sus siglas en inglés) permite conectar a las personas y entregar la información correcta a la persona indicada, en el momento oportuno, a través del análisis de la data más útil para la toma de decisiones.

El usuario también ha cambiado a la par de los avances tecnológicos. Este busca estar conectado, autónomo, exigente, participativo, multicanal y multidispositivo. Además, tiene expectativas elevadas en cuanto a la experiencia en los canales digitales y la posibilidad de interactuar con las instituciones financieras 24/7 (ver Gráfico 9). Estas mejoras han generado un incremento en la oferta de servicios financieros donde ahora no solo participan las instituciones financieras tradicionales sino también actores nuevos que están aprovechando la tecnología para acercarse a los clientes, brindando una mejor experiencia y dándoles la oportunidad de tener un banco en sus manos.

Gráfico 9: Los nuevos usuarios digitales

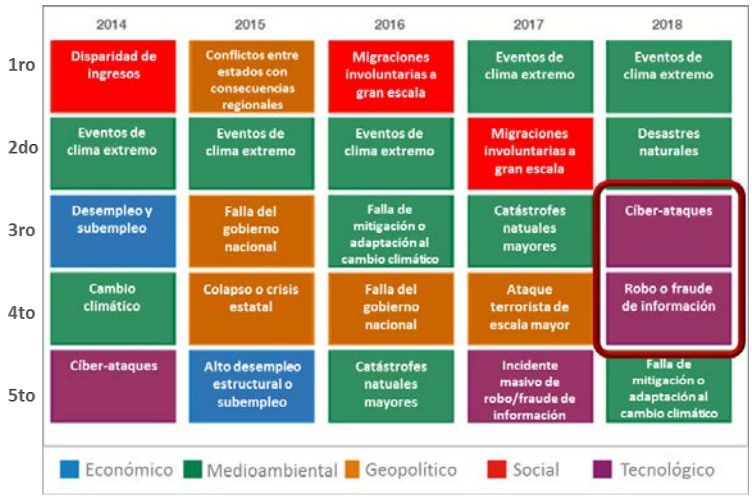


Fuente: *KPMG, El nivel de madurez digital, abr. 2017*

Los riesgos de la era digital

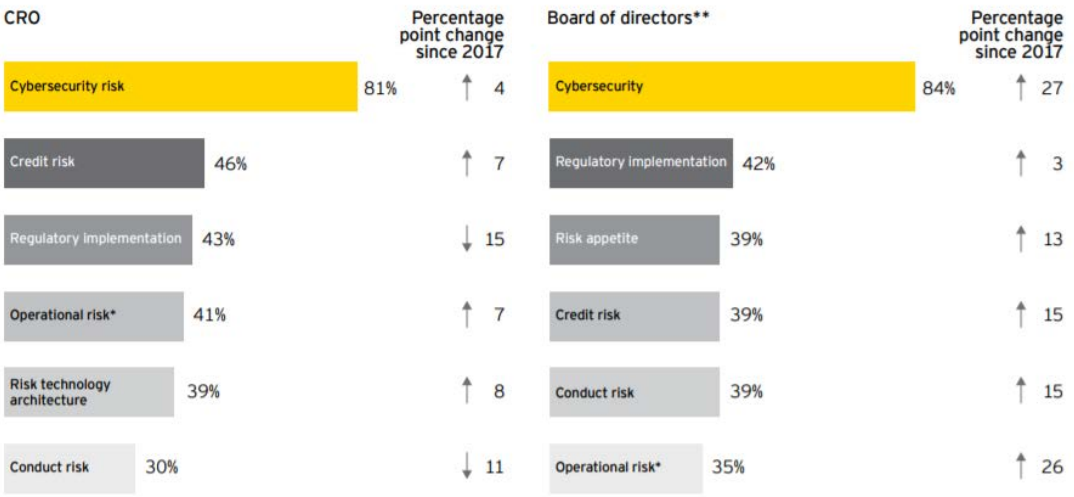
La ciberseguridad se ha convertido en el segundo riesgo más importante luego de eventos relacionados a desastres naturales, según el Foro Economico Mundial (ver Gráfico 10). Además, en una reciente encuesta de EY al sistema financiero, la ciberseguridad es el riesgo que permanece como tema principal en las agendas de los directores de riesgo (CRO, por sus siglas en inglés) y los directorios en el mundo (ver Gráfico 11). Esto refleja que las amenazas cibernéticas son uno de los riesgos emergentes que ha ido tomando mayor peso en los últimos años a raíz de los distintos ataques a diversas industrias estratégicas a nivel mundial.

Gráfico 10: Clasificación de riesgos



Fuente: *Foro Económico Mundial*

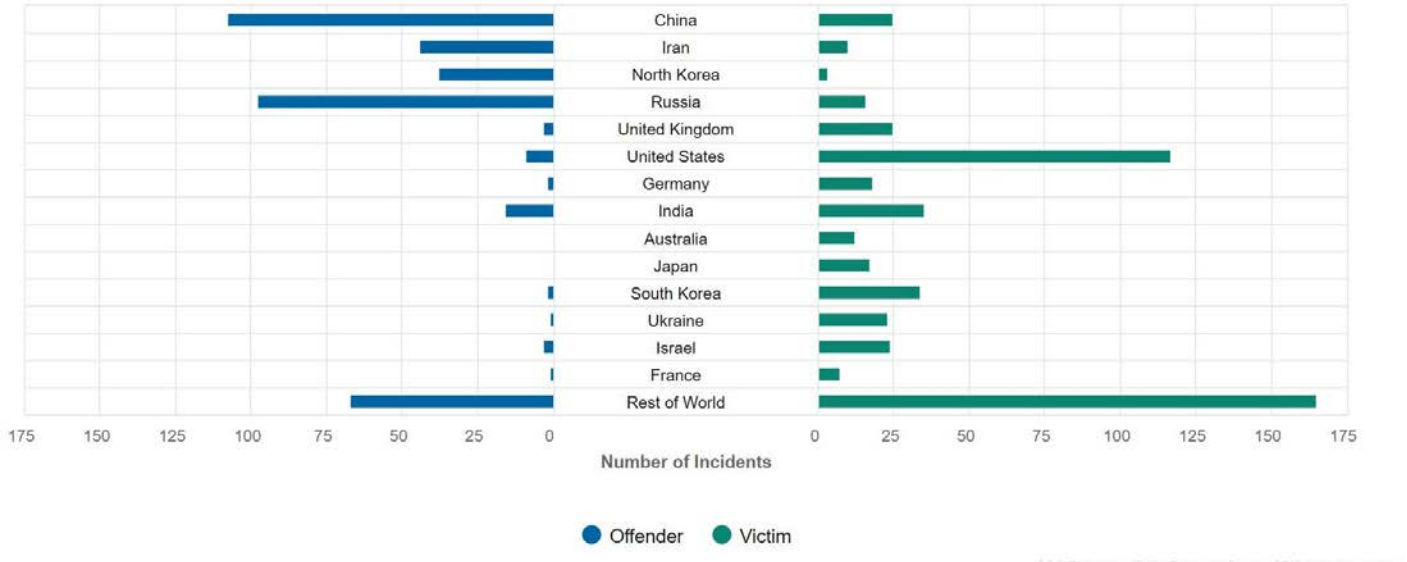
Gráfico 11: Principales prioridades de riesgo en los próximos 12 meses



Fuente: *Ninth annual EY/IIF Global Bank Risk Management Survey*

Esta preocupación se genera a raíz de los eventos registrados en los últimos años en distintas industrias (energía, entidades financieras, etc.) y entidades del gobierno. Se estima que el costo del ciberdelito al 2021 llegará a USD 6 billones al año (el narcotráfico genera pérdidas por USD 1 billón)[90]. Las pérdidas corresponden al costo directo de reparación de daños una vez ocurrido el ataque (recuperación de información y recursos, reparación de activos, etc.) y los costos indirectos que incluyen las horas extra necesarias para la revisión de seguridad, lo cual conlleva a un impacto en la productividad de los equipos, y los costos legales/reputacionales luego del incidente (multas, juicios, reducción del precio de la acción por impacto reputacional). Además, es importante agregar que existe un costo de mediano/largo plazo que consiste en el cambio en el comportamiento del cliente (recuperación de confianza, seguridad en la marca e incluso participación de mercado luego del ataque) que es difícil medir y donde aún no se tiene una estimación clara del costo (ver Gráfico 12).

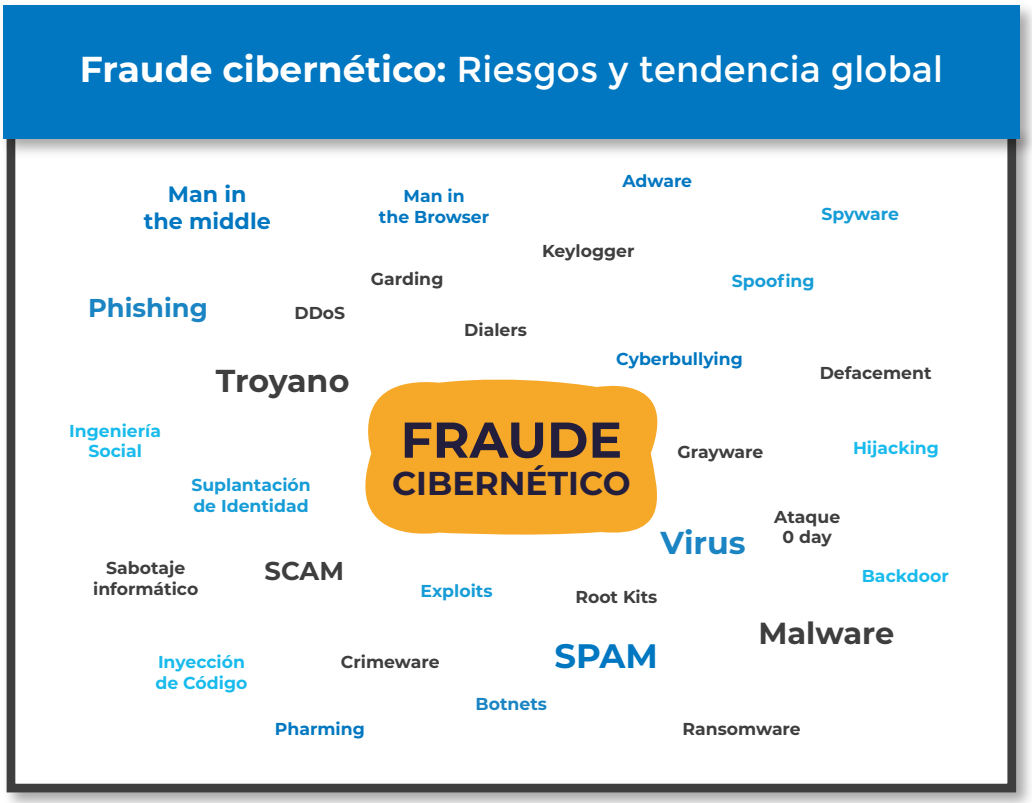
Gráfico 12: Número de ciberataques por país



Fuente: *CSIS & Hackmageddon*

Las amenazas se pueden clasificar en cuatro grupos: i) Ciber extorsión: cuando el sistema informático se somete a acciones o amenazas con la negación reiterada de servicio u otros ataques donde los hackers exigen dinero para detener los ataques u ofrecer protección (el caso más conocido es el ransomware); ii) Ciberfraude: donde se realiza un fraude mediante la manipulación de los sistemas informáticos (por ejemplo, cuando se suplanta la identidad de los clientes a través de ataques de *phishing*, vishing, etc); iii) Ciberguerra: ataques sofisticados dirigidos a gobiernos (en estos casos se cuenta con financiamiento y recursos sofisticados); y iv) Ciberterrorismo: se realizan ataques terroristas mediante la utilización de recursos informáticos y el ciberespacio (Anonymous). Los dos primeros están relacionados con amenazas al sistema financiero; asimismo, la tipología de los ataques puede estar dirigida a las instituciones financieras o directamente al cliente (ver Gráfico 13).

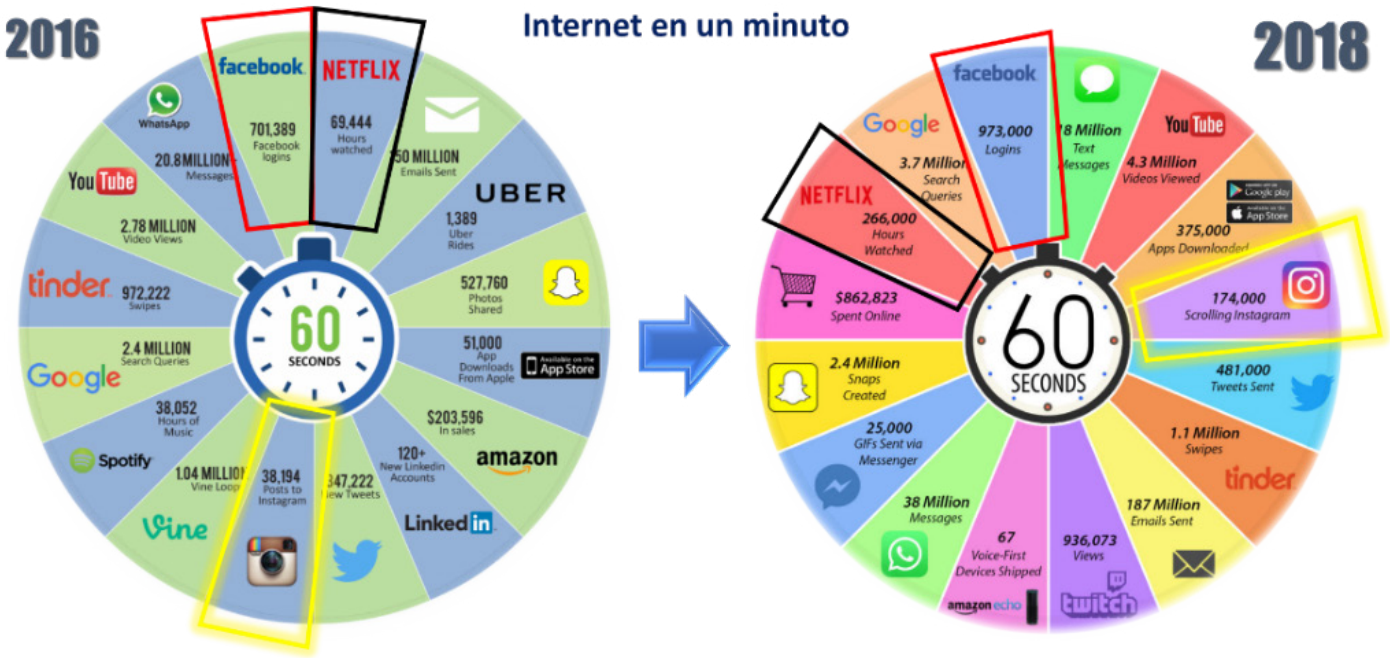
Gráfico 13: Principales riesgos cibernéticos



Fuente: *Elaboración propia*

Los avances tecnológicos mejoran la experiencia del cliente; los usuarios interactúan cada vez más con los aplicativos (ver Gráfico 14), generando información para que las empresas puedan ofrecerles servicios especializados. Asociado a estas mejoras en la oferta comercial también existe el riesgo de que esa información caiga en manos de ciberdelincuentes y sea utilizada para cometer fraude cibernético (por ejemplo, a través de la suplantación de identidad). A medida que la tecnología evoluciona también se desarrollan nuevas y sofisticadas amenazas cibernéticas, por lo que es necesario estar preparados en el manejo de la crisis cibernética, evaluando los riesgos y creando resiliencia dentro de la organización. Finalmente, el uso de analítica de datos y tecnología tiene que guiar la gestión de manejo de riesgos para hacer frente a las nuevas amenazas. La mayoría de los bancos considera que el desarrollo de nuevas tecnologías será utilizado para el monitoreo del fraude y para el crimen financiero (monitoreo del fraude - 72%, crimen financiero: 68%)[91].

Gráfico 14: Internet en un minuto



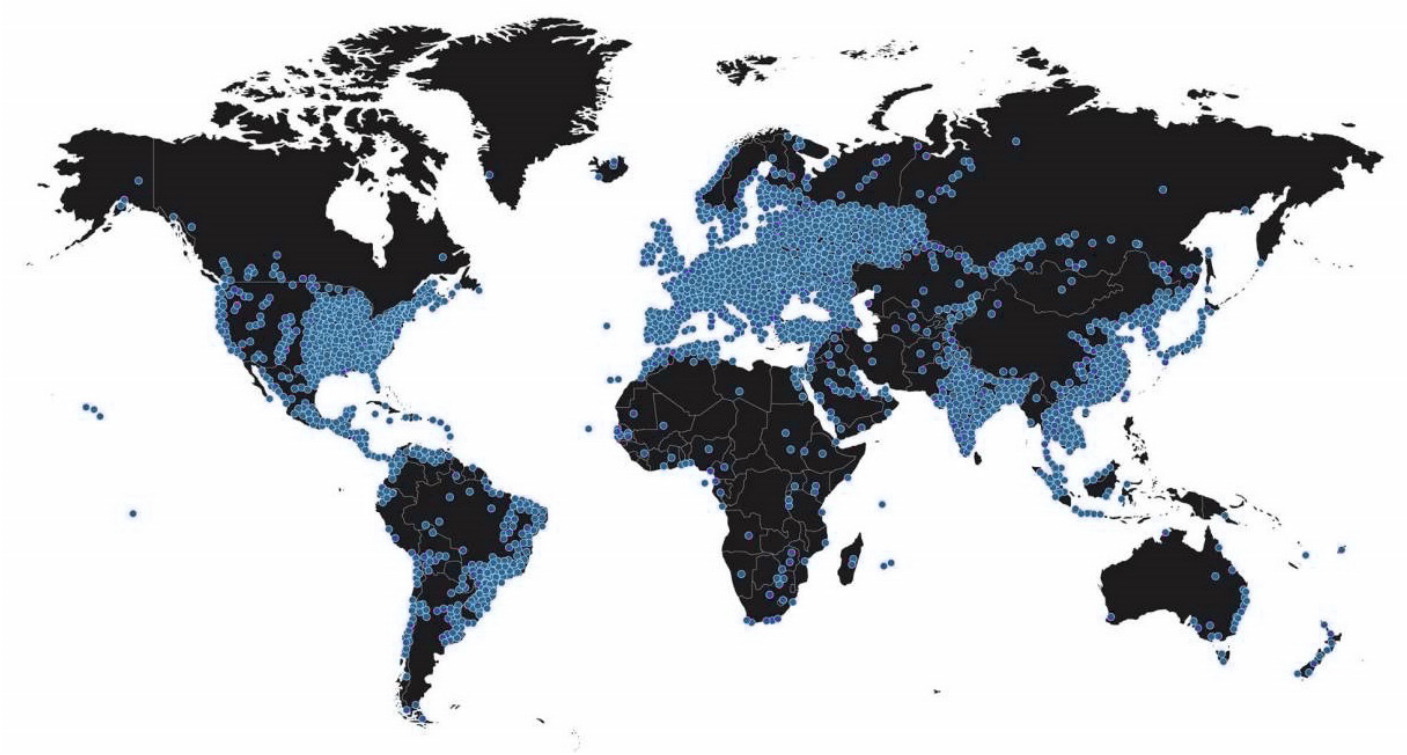
Fuente: *Digital Information World*

El ciberespacio da pie a que la información esté disponible para personas comunes. La web de superficie es solo el 10% del contenido web; el 90% de la información se encuentra en la "web profunda" en un ambiente no regulado, donde los ciberdelincuentes tienen acceso a información personal de los clientes, lo cual permite que los ataques puedan ser automatizados y dirigidos, generando mayor impacto con un nivel de esfuerzo más reducido.

Las reglas de juego, construyendo al revés y a baja velocidad

Distintas organizaciones han sido víctimas del ciberdelito en los últimos años. A la fecha los ataques más conocidos y de mayor impacto tanto financiero como reputacional han sido los *ransomware* de Petya y Wannacry donde se mantuvo información relevante cautiva a cambio de una recompensa monetaria afectando operaciones de conocidas empresas a nivel mundial como: Telefónica, FedEx, Nissan, Bank of China, Petrobrás, etc. Wannacry infectó alrededor de 15 millones de equipos alrededor del mundo (ver Gráfico 15), mientras que Petya tuvo un impacto en más de 60 países. Al sumar ambos eventos, se estima que las pérdidas podrían llegar a los 8 billones de USD[92].

Gráfico 15: Impacto de Wannacry



Fuente: *Deloitte*

Por otro lado, existen otros ciberataques que buscan robar información personal de las personas para luego venderlas en la web profunda con el objetivo de hacer fraude fiscal, suplantación de identidad, entre otros. Este tipo de ataques tiene un impacto de más largo alcance ya que la información personal no suele modificarse de forma inmediata y no es fácil para una institución darse cuenta de que ha sido víctima del robo de información de clientes. El atacante tiene mayor tiempo para poder armar la estrategia de ataque. Uno de los ataques de este tipo más conocido fue el que reconoció Equifax en el 2017 donde se comprometió información de 143 millones de consumidores estadounidenses.

Los ataques continúan enfocándose a organizaciones privadas, gubernamentales y activos críticos de información, donde nadie es inmune a los ciberataques. Considerando este contexto y las necesidades del mercado, los entes regulatorios en el mundo actuaron de forma reactiva luego de los distintos eventos, dando lineamientos sobre cómo proteger la información y reconociendo que aún falta mucho por explorar.

En la Unión Europea se aplicó la Reglamento General de Protección de Datos (GDPR, por sus siglas en inglés) efectiva a partir de mayo 2018, donde el consumidor tiene que darles consentimiento a las empresas que quieran utilizar su información personal para fines comerciales. En cualquier momento el consumidor podrá quitar ese consentimiento y decidir transferir la información a otra organización. Las multas asociadas a infringir esta regulación podrían llegar a 20 millones de Euros o 4% de la facturación global (el mayor de los dos)[93].

Estados Unidos, a raíz de los ataques, publicó en agosto de 2018 un documento con la Estrategia Nacional de Ciberseguridad (*National Cyber Strategy*)[94] destacando este tema como foco a nivel de estado. Además, el mismo mes, el Departamento de Servicios Financieros de Nueva York (NYDFS) publicó la

regulación de ciberseguridad (23 NYCRR 500) estableciendo su primera fecha límite de cumplimiento para 1.500 bancos e instituciones financieras. La regulación indica que las empresas financieras tienen que informarle al NYDFS de cualquier incidente de ciberseguridad, con un plazo no mayor de 72 horas. Además, se definieron distintas políticas que deberán implementarse según el plan de adecuación hasta marzo de 2019, donde se busca contar con un plan de ciberseguridad robusto liderado por el CISO que se encargará de revisar los procesos de seguridad de la información y el mantenimiento de los mismos. Finalmente, se definió la implementación de controles efectivos para prevenir acceso no autorizado a información de los sistemas o información no pública. Los controles pueden incorporar autenticación multi-factor, biométrica o en base a riesgo.

Complementario a los mandatos de la Unión Europea y EE. UU. mencionados, se publicaron distintos requerimientos enfocados en pagos digitales. El PSD2 (Payment Services Directive 2 – EU) y el PCI DSS (global Payment Card Industry Data Security Standard) son requerimientos dirigidos para los bancos y autorizadores donde se exigen procesos de autenticación más robustos para proteger a los clientes. Las pautas de autenticación incluyen: i) autenticación basada en dos o más factores (claves, biometría, etc.); ii) análisis de riesgo transaccional; iii) enlace dinámico y iv) seguridad para dispositivos móviles comprometidos (protección de replicación).

En Latinoamérica, los reguladores han tenido iniciativas relacionadas con la protección de datos personales como en Brasil donde en julio de 2018 se publicó la Ley N.° 53-2018 relacionada a este ámbito y en Chile, que en agosto de 2018 emitió la Ley N.° 19620, además de crear una agencia responsable de la protección de datos a nivel nacional. Estos esfuerzos vienen dándose de forma reactiva en el proceso de transformación, sin incluir cuáles son las vulnerabilidades que las instituciones financieras deben atender para proteger a sus clientes de estas nuevas amenazas.

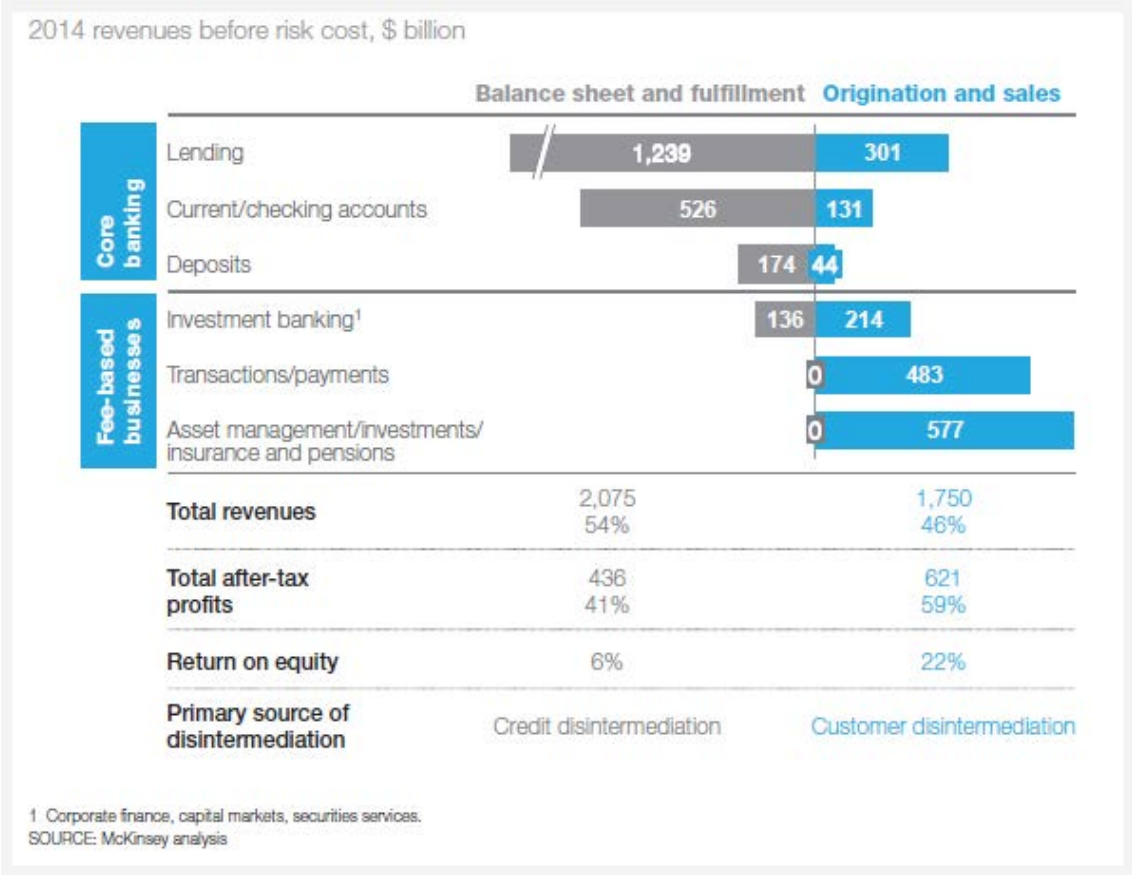
Si bien es cierto que la banca es una industria amplia y detalladamente regulada, para hacer frente a los riesgos emergentes es preciso activar permanentemente la capacidad de autorregulación para enfrentar especialmente los riesgos cibernéticos de forma preventiva, y no reactiva como han actuado los reguladores. Es importante fijar estándares con permanente pauta de revisión ante los factores de escalabilidad, tecnología de última generación (robótica, inteligencia artificial, etc.) y constante evolución de las tipologías de los ataques. El objetivo debe incluir dar respuestas rápidas a los ataques cibernéticos permitiendo que los servicios que prestan no se vean interrumpidos y protegiendo la información de los clientes, fortaleciendo las capacidades de identificación, contención, prevención, respuesta y recuperación.

C. Vientos de cambio y nueva visión

Un viento estratégico, innovación, apetito de riesgo y seguridad

El 60% de las utilidades del sistema financiero ya no se generan por el *core* bancario, la intermediación generada por activos y pasivos, ahora se concentra en las operaciones transaccionales, la gestión del portafolio, los seguros y pensiones. Lo anterior es consecuencia del impacto de la digitalización y la intrusión de nuevos actores en el ecosistema financiero en un proceso acelerado de transformación continua que las organizaciones vienen enfrentando.

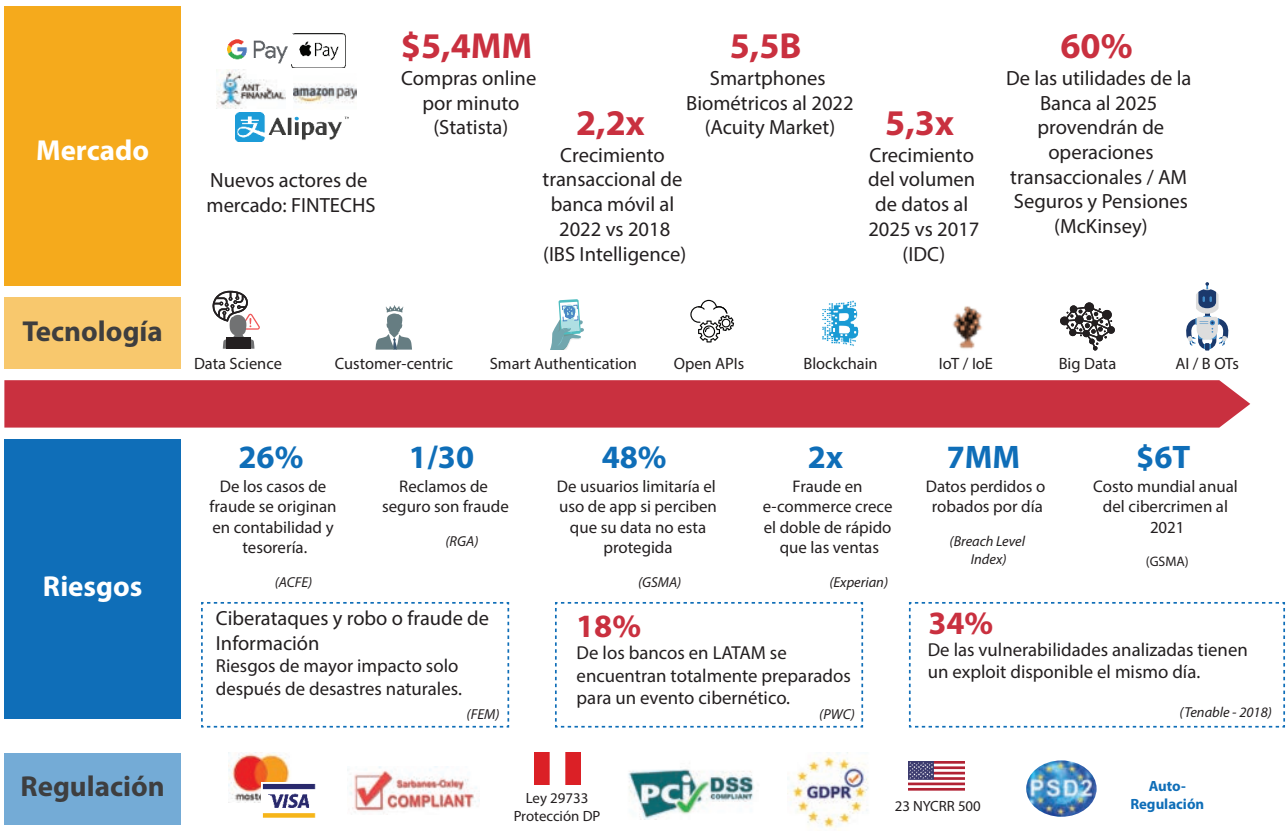
Gráfico 16: Distribución de utilidades al 2014



Fuente: *The future of bank risk management – 2014. Mckinsey.*

Debido a esta transformación, se presentan nuevos vectores de vulnerabilidad en el día a día con impacto hacia todos los activos (financieros, marca e información). Solo como muestra están las brechas de datos a nivel mundial que generan 7MM de datos perdidos o robados al día[95], o la proyección del costo anual del ciberdelito de $6T al 2021 (ver Gráfico 17). La evolución de la criticidad de los riesgos de ciberseguridad nos llama a redefinir las estrategias de respuesta ante ataques cibernéticos, gestionando el riesgo desde su transferencia, mitigación, evasión o incluso su aceptación; y nos llama a adoptar innovación, talento e intercambio de información para enfrentar a este nuevo ecosistema digital que permita empoderar al negocio a innovar, a la vez que fomentar la seguridad bajo una nueva visión.

Gráfico 17: Evolución del mercado, tecnología, riesgos y regulación

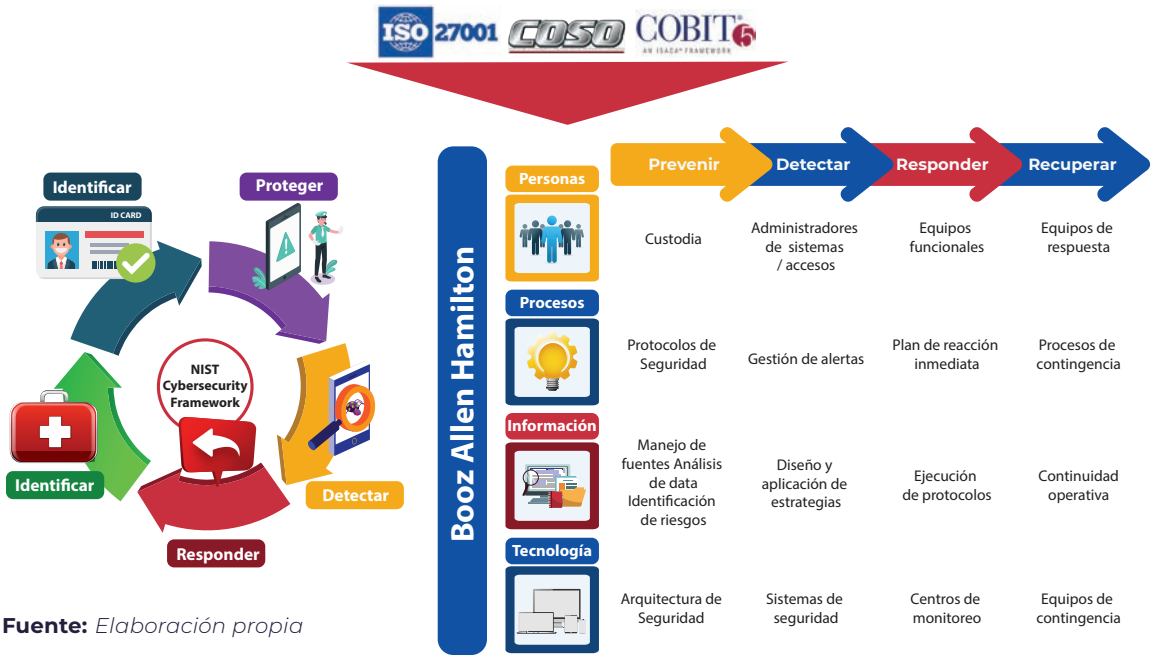


Fuente: *Elaboración propia*

El modelo que se establezca para la protección de los activos debe permitir coordinar las acciones entre las unidades aliadas en la gestión del riesgo cibernético. La implementación de diversos marcos metodológicos como NIST, COSO, COBIT, estándares internacionales, entre otros, contribuyen a esta tarea al definir los ejes con los que el modelo debe contar y al ser una guía respecto de los controles necesarios, permitiendo la autorregulación de las entidades sin la dependencia de la normativa de los reguladores que no siempre es comunicada de forma oportuna. Tomando esto en consideración, la estrategia de ciberseguridad debería enmarcarse en la gobernanza y definición del apetito de riesgo de la organización, incluyendo los enfoques y procesos de prevención, detección, respuesta y recuperación ante los ataques cibernéticos que permitan mantener un nivel adecuado de protección (ver Gráfico 18).

Gráfico 18: Implementación de un modelo de prevención basado en un marco de trabajo

Implementación de un Modelo de Prevención de Fraude Cibernético basado en un Marco de Trabajo Estándar



Fuente: *Elaboración propia*

Bajo el enfoque de gobernanza, es relevante que la alta dirección esté conciente respecto de la criticidad de los riesgos de ciberseguridad para que pueda liderar y mostrarse comprometida en la gestión sobresaliente de los riesgos y eventos que se materialicen. De esa forma, las políticas, roles, comités y *accountability* que se generen respecto a este frente podrán cobrar importancia en la organización para una efectiva toma de decisiones. De lo contrario, no se tendrá influencia en los cambios requeridos para ejecutar la estrategia de ciberseguridad.

Asimismo, la toma de decisiones deberá basarse en el apetito de riesgo que la organización defina para sus activos, productos y procesos críticos previamente identificados, y así, dirigir los esfuerzos de la gestión de riesgos de ciberseguridad hacia los niveles que el directorio apruebe.

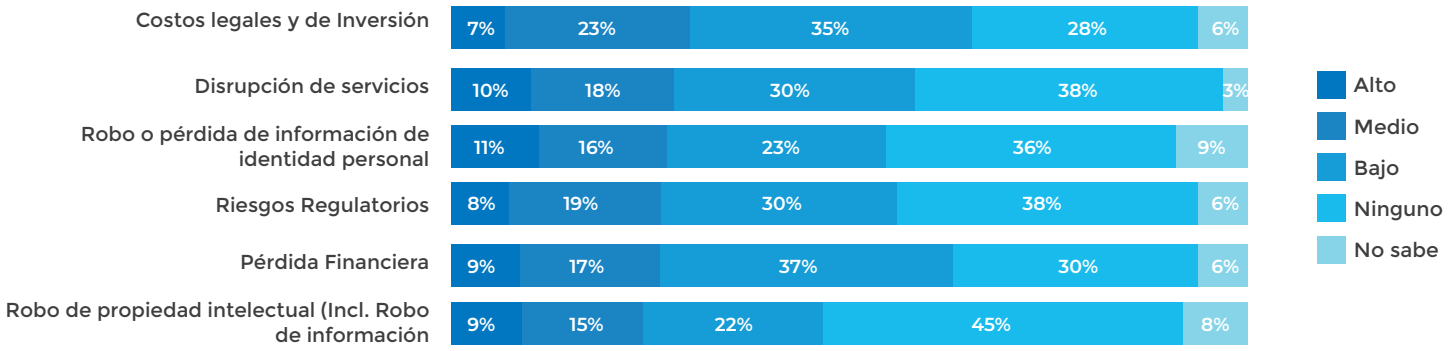
Respecto del proceso de prevención, existen diversos focos de trabajo en los cuales concentrarse para lo que es vital en la identificación y coordinación con aliados claves dentro de la organización: recursos humanos, sistemas, cumplimiento, líneas de negocio, incluso proveedores y expertos externos. Las actividades de cultura y aprendizaje para el entrenamiento continuo del personal y clientes; la evaluación preventiva de riesgos de ciberseguridad tanto en procesos críticos como en la incepción de nuevos productos digitales, su correcta valorización y tratamiento; la implementación de sistemas inteligentes de autenticación y la generación de protocolos ante eventos de ciberseguridad son algunos de los procesos que permiten contar con una estrategia preventiva para la mitigación de los riesgos de ciberseguridad.

De acuerdo con el estudio EY Global Banking Outlook 2018, la primera prioridad de los bancos en este proceso de transformación digital es mejorar la protección y seguridad de los datos (ver Gráfico 19), debido a que la información viene siendo uno de los principales activos para la digitalización y personalización de los servicios bajo el enfoque centrado en el cliente. El objetivo es detectar de forma oportuna los ataques dirigidos y compromisos de información para reducir el impacto financiero, reputacional y legal que un ciberataque conlleva (ver Gráfico 20).

Gráfico 19: Prioridades de los bancos en la era digital

Fuente: *Elaboración propia*

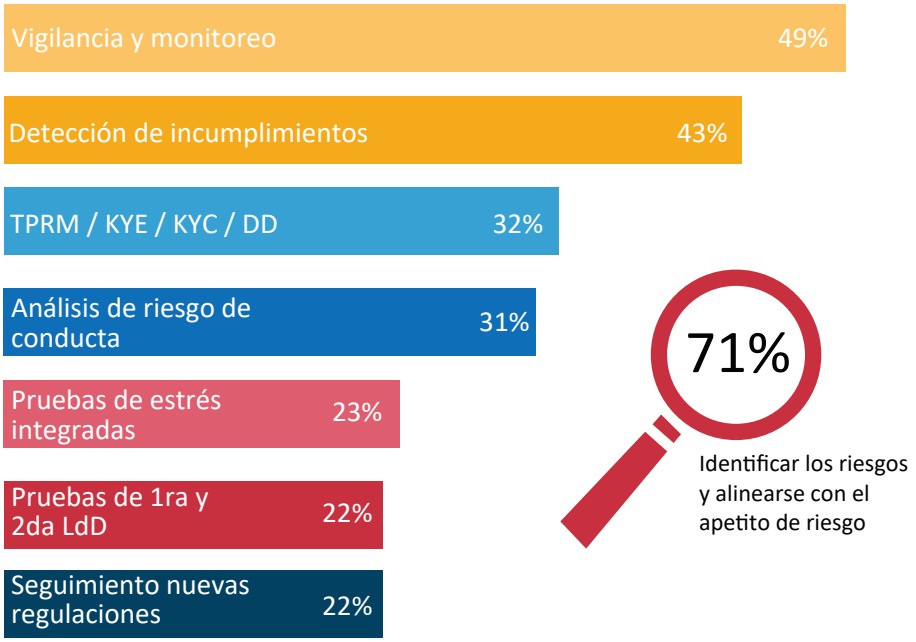
Gráfico 20: Impacto de los ciberataques



Fuente: *PriceWaterhouseCoopers*

La transformación digital ha impactado, hoy día, en la gestión de riesgos, de manera tal que los bancos esperan digitalizar actividades centrales como vigilancia y monitoreo aprovechando sobre todo los esfuerzos en la explotación de la información (ver Gráfico 21). Es así que el proceso de detección requiere de alta inversión en tecnología avanzada que permita contar con monitoreo de amenazas en tiempo real, uso de modelos de aprendizaje automático y grandes datos con mayor precisión, integración y correlación de fuentes de información para una visión integral 360°, entre otras funcionalidades. Lo descrito anteriormente requerirá de cambios y corrección de vulnerabilidades en la infraestructura tecnológica, muchas veces obsoleta.

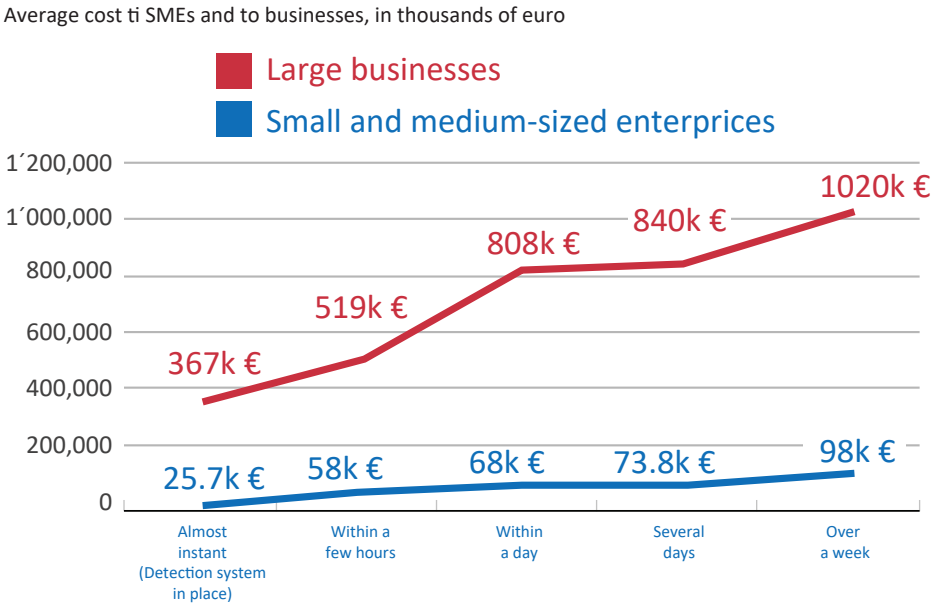
Gráfico 21: Procesos de alto riesgo y cumplimiento que se digitalizarán en el 2018



Fuente: *2017 Risk Management Global Sruvey*

No generar iniciativas en este frente producirá un incremento significativo en el costo del ciberataque, al duplicarse el tiempo de detección, de horas a una semana (ver Gráfico 22).

Gráfico 22: Impacto de ciberataques acordes con el tiempo de detección



Notes: Survey of 4,000 business representatives from 25 countries

Fuente: *Karpersky Lab, "Measuring Financial Impact of IT Security on Businesses",2016*

La probabilidad de que un ciberataque ocurra en las organizaciones, o incluso ya esté ocurriendo sin ser notado, es alta. Por ello, establecer procesos robustos de respuesta y recuperación son una prioridad para contener el impacto de la materialización de los riesgos de ciberseguridad. Algunos puntos a tener mapeados son el establecimiento de equipos, planes de contingencia y protocolos para asegurar la continuidad operativa, la validación y prueba de estos planes ante la vulneración de controles, incluyendo la respuesta a ataques día cero y la gestión de crisis, nuevamente involucrando a las unidades aliadas en el modelo de seguridad adoptado por la organización.

Viento de integración con información, enfoque global

La transformación digital que está alcanzando creciente ímpetu y relevancia en el sistema financiero de Latinoamérica viene acompañada de nuevas amenazas y riesgos, pero también de nuevas oportunidades latentes que las organizaciones proactivas pueden explotar para hacer frente al nuevo escenario de riesgo cibernético. Tal como sucedió en su momento con la electricidad en la revolución industrial, los datos y el Internet se volverán un sustrato que estará a la vez en todos lados y del cual dependerán todos los procesos y actividades a nivel empresarial e industrial.

El Internet de la cosas o su segunda derivada, el internet de todo, implica la interconexión mediante sensores, API y motores de información compartida de manera constante y a tiempo real, que junto a nuevas ramas de investigación científica como la ciencia de los datos, el aprendizaje de máquinas y la inteligencia artificial permitirán generar inteligencia de una manera nunca antes vista. De igual manera, el gestor de riesgos cibernéticos debe prepararse para apalancar el avance en estas tecnologías y el conocimiento requerido para implementarlas.

Por un lado, las API abiertas y la interconectividad de herramientas de monitoreo y de canales de negocios fomentará una mayor disponibilidad de información de los clientes y eventos cibernéticos desde una perspectiva omnicanal y a tiempo real. Esto puede ser explotado para la generación de modelos de perfil de cliente y de comportamientos anómalos que permita una pronta detección de riesgos cibernéticos. La mayor centralización y completitud de la información es también favorable para el rol de respuesta forense ya que permite una reconstrucción de los incidentes cibernéticos para una respuesta más rápida y subsanación más completa de las vulnerabilidades. La inteligencia generada por este proceso puede retroalimentar la inteligencia de la organización, tanto para identificar como para prevenir este tipo de incidentes a futuro, bajo una función inmunizadora del riesgo específico.

Esta capacidad de inteligencia para la prevención de materialización de riesgos cibernéticos se potencia exponencialmente al apalancar la generación de conocimiento y cooperación colectiva. Por un lado, el compartir información de amenazas a nivel gremial, inter-industrial y bajo un enfoque global mediante plataformas centralizadas y comisionadas, se cumple un doble rol de prevenir el impacto en la organización ante un vector de ataque cibernético latente identificado en otra entidad, permitiendo generar soluciones de manera prospectiva y una más rápida identificación y priorización de vulnerabilidades. Por otro lado, se genera también una situación disuasoria ante el ciberatacante dado que limita la escalabilidad de los ataques haciéndolos un negocio menos atractivo y rentable. Esto se traduce en una función inmunizadora a nivel industrial que disuade efectos de contagio que podrían generar una pérdida de confianza en el sistema financiero generando un daño colateral a todas las instituciones financieras[96].
Complementariamente, es de creciente importancia generar comunidades de conocimiento:

- A nivel gremial e interindustrial, fomentando la generación de soluciones a problemas y amenazas a través del esfuerzo coordinado. Podría, por ejemplo, generarse inteligencia complementaria para la mitigación del riesgo como un puntaje de riesgo cibernético de un cliente a nivel industrial.

- A nivel académico, para fomentar el desarrollo de las capacidades necesarias por la industria financiera en el ámbito de seguridad cibernética, para impulsar la incubación y desarrollo de emprendimientos complementarios a la ciberseguridad y otras iniciativas que puedan responder a problemas de la industria.

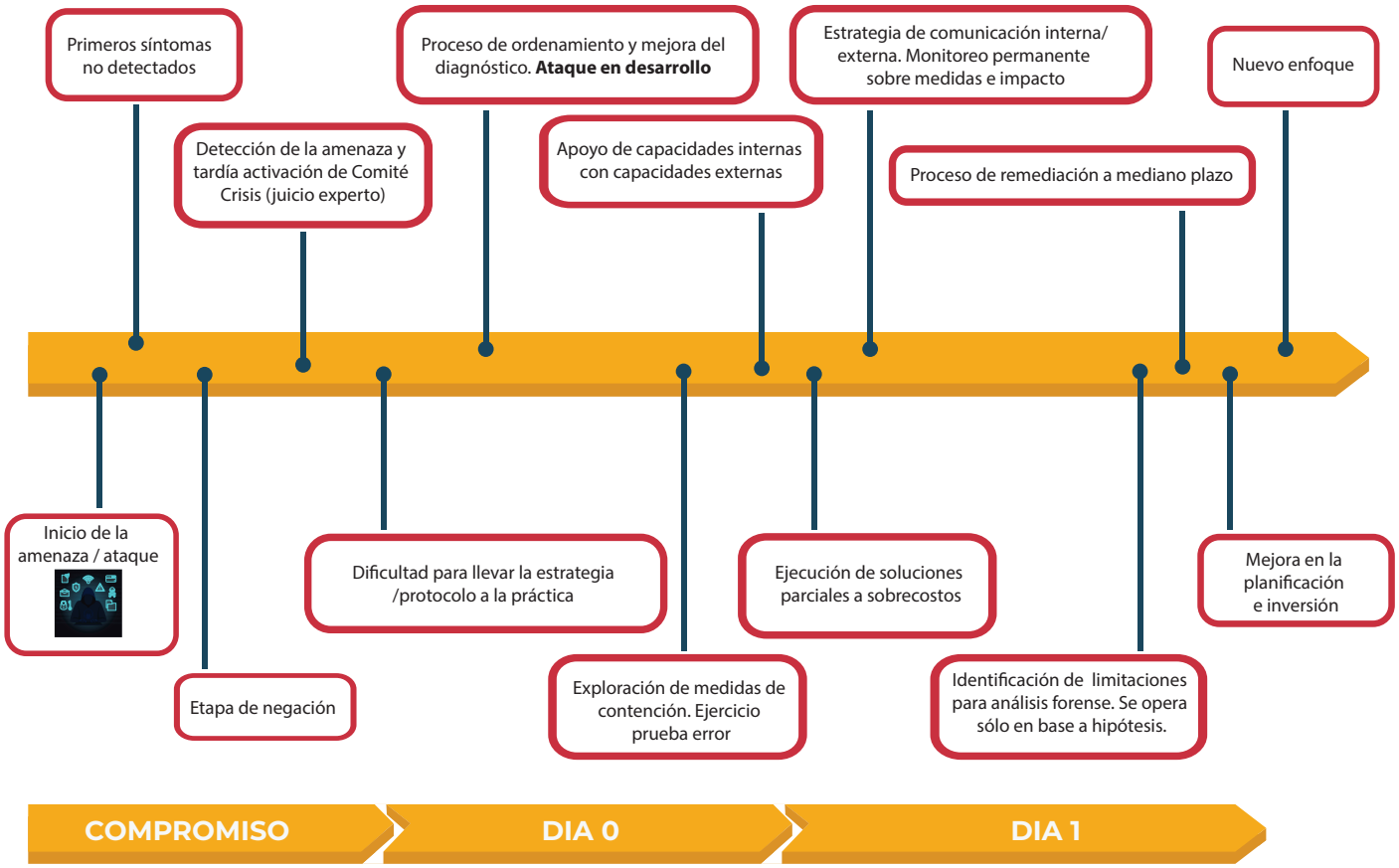
- A nivel gubernamental, para fomentar la idoneidad de la regulación que acompañe la evolución de las amenazas sin frenar la innovación del sector financiero; para fomentar la cooperación de ámbitos clave como las fuerzas del orden público y el sistema judicial que conlleve a una penalización efectiva de los ciberatacantes bajo un rol punitivo, de resarcimiento y disuasorio. Igualmente, para apalancar la información o inteligencia estatal para la prevención de riesgos cibernéticos (registros gubernamentales de biometría, por ejemplo).

- A nivel social, fomentar la inclusión de materias en función de la ciberseguridad y ecosistema digital para luchar contra el 'analfabetismo digital' que es una problemática compartida en la región y así poder reclutar a los clientes en la lucha contra las ciberamenazas y sean menos susceptibles a ataques como el *phishing* o ingeniería social[97].

Cerrando la brecha

Estudiando la respuesta típica de una organización ante un ataque cibernético se puede identificar una problemática común para la gestión de los riesgos cibernéticos, permitiendo identificar varios frentes de mejora (ver Gráfico 23).

Gráfico 23: Manejo de crisis: problemática común para la gestión



Fuente: *Elaboración propia*

Por un lado, como se señaló, se deben potenciar las capacidades de detección implementando tecnologías de analíticas de datos que incluyan tecnologías de aprendizaje automático e inteligencia artificial basado en grandes datos, que permitan mejorar la detección y poder generar modelos de riesgo cibernéticos que evolucionen a la par de las nuevas amenazas. Debe generarse una labor prospectiva de las nuevas amenazas, necesidades y tecnologías en el ecosistema digital y financiero para generar y sustentar proyectos de renovación de tecnología, captura de talento e implementación de nuevas metodologías de avanzadas que preparen a la organización ante los nuevos riesgos.

Complementariamente es importante pensar en contingencia, pues es inevitable que en algún momento, algún control será vulnerado y podrá ocurrir un compromiso o intrusión. Es imperativo producir simulaciones de ataques que sean integrales, inteligentes y adversarios que permitan probar los protocolos y estrategias de protección de los activos críticos; que posibiliten identificar puntos de mejora en la información disponible para análisis forense; y que muestren las capacidades actuales de respuesta frente a estos eventos para evidenciar las limitaciones y necesidad de expertos externos disponibles. No debe esperarse la materialización de un ataque para generar lecciones aprendidas y optimizar los planes de respuesta.

Asimismo, toda organización debería realizar la debida diligencia en iniciar una evaluación de su nivel de madurez respecto de la seguridad cibernética y niveles inherentes y residuales de riesgo que permita identificar y priorizar esfuerzos de mejora[98].

Finalmente, debido al nivel especializado y escaso talento para el cumplimiento de estas funciones, es clave fomentar la capacitación y programas de desarrollo de personal debido a la dificultad de encontrar perfiles con todas las cualificaciones requeridas en el rol. Complementariamente, debido al continuo avance en la tecnología, herramientas y conocimientos en este ámbito, se debe fomentar y requerir la constante actualización de conocimientos y la participación activa en el ambiente de intercambio de conocimiento industrial y académico.

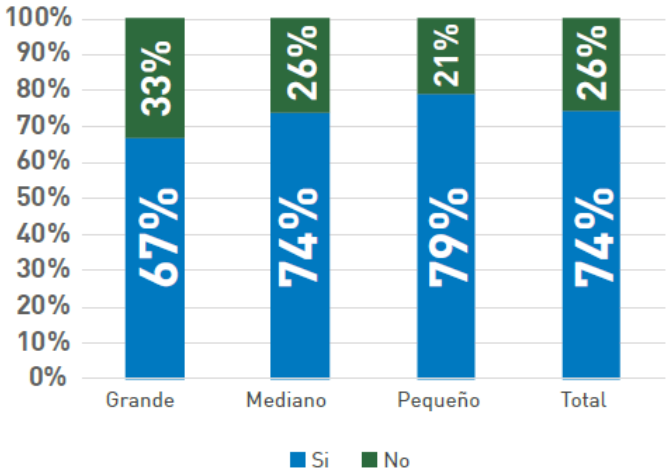
Lo cuantitativo y cualitativo: Estudio del Estado de la Ciberseguridad en el Sector Bancario en América Latina y el Caribe. Principales aportes.

Gracias al estudio del Estado de la Ciberseguridad en el Sector Bancario en América Latina y el Caribe, elaborado por la Secretaría General de la Organización de los Estados Americanos (OEA), se logró cuantificar el nivel de conciencia, el avance y las necesidades del sistema financiero respecto a las crecientes amenazas de este frente, generando puntos de referencia en la región que serán parte de la justificación de próximas iniciativas contra los ciberataques que proponga cada organización.

Resaltamos algunos de los principales hallazgos del estudio, en relación al costo del riesgo de ciberseguridad, gobierno, procesos y características de los ataques recibidos en la región. En caso de requerir mayor detalle sobre el tema, el lector puede acudir al sitio oficial de la OEA donde se encuentra el informe original.

En relación con la preparación y gobernanza de la seguridad digital, en promedio, en el 74% de las entidades bancarias se tiene un único responsable de la seguridad digital. El porcentaje restante tiene hasta 3 áreas para el cumplimiento de este rol (ver Gráfico 24). En promedio, el total de colaboradores que las organizaciones tienen en esta función es de 49 personas en un banco grande, 16 en un banco mediano y 4 en banco pequeño, con miras a mantener ese tamaño en el corto plazo según el 82% de los encuestados.

Gráfico 24: Área única responsable de la seguridad digital en la entidad bancaria



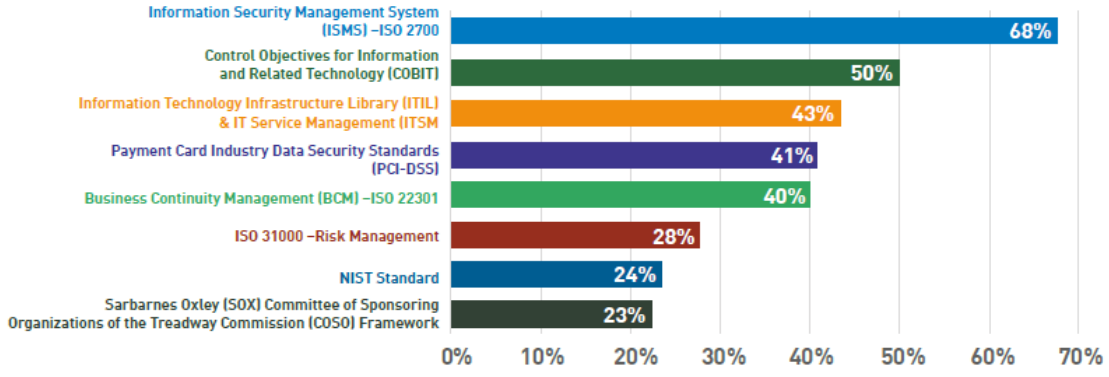
Nota: 191 registros

Fuente: *SG/OEA a partir de la información recolectada de entidades bancarias en América Latina y el Caribe*

El estudio también resalta la necesidad del apoyo de la alta dirección respecto a los esfuerzos en ciberseguridad, que vienen dando mayor prioridad a los proyectos de este frente, según diversos especialistas como EY e ISACA.

Respecto a la preparación de las entidades, se evidencia la adopción de marcos de seguridad y/o estándares internacionales relacionados a ciberseguridad, siendo las más implementadas el estándar Information Security Management System (ISO 27000), el marco de trabajo Control Objectives for Information and Related Technology (COBIT) y los conceptos y buenas prácticas señaladas por el Information Technology Infraestructure Library (ITIL) & IT Service Management (ITSM) (ver Gráfico 25).

Gráfico 25: Marcos de seguridad y/o estándares internacionales adoptados



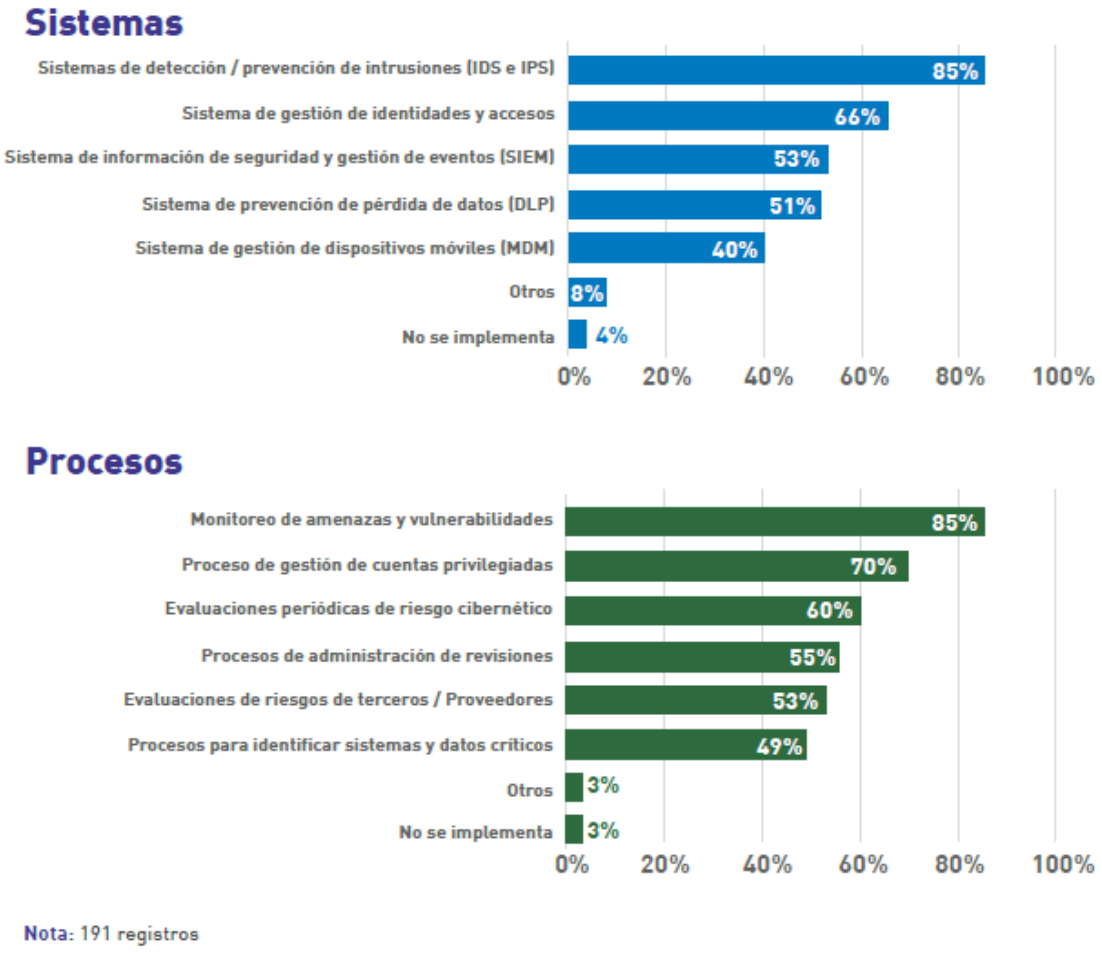
Nota: 191 registros

Fuente: *SG/OEA a partir de la información recolectada de entidades bancarias en América Latina y el Caribe*

Sobre los procesos y controles implementados relacionados a seguridad digital, más del 50% de las entidades encuestadas cuentan con sistemas de detección y prevención de intrusiones (IDS e IPS), sistema de gestión de identidades y accesos, sistema de información de seguridad y gestión de eventos (SIEM, por sus siglas en inglés) y de prevención de pérdida de datos (DLP, por sus siglas en inglés). Estas

herramientas refuerzan principalmente el proceso de monitoreo de amenazas y vulnerabilidad y gestión de cuentas privilegiadas. Quedan más relegados procesos clave como la identificación de sistemas y datos críticos que ayuden a la generación de estrategias y tácticas priorizadas de ciberseguridad y las evaluaciones de riesgo de terceros/proveedores, a pesar de la creciente tercerización de personal en procesos críticos como el desarrollo de nuevos productos y administración de sistemas, donde podrían tener acceso a información restringida poniendo en riesgo su confidencialidad, disponibilidad e integridad (ver Gráfico 26).

Gráfico 26: Herramientas, controles y procesos implementados en la entidad bancaria

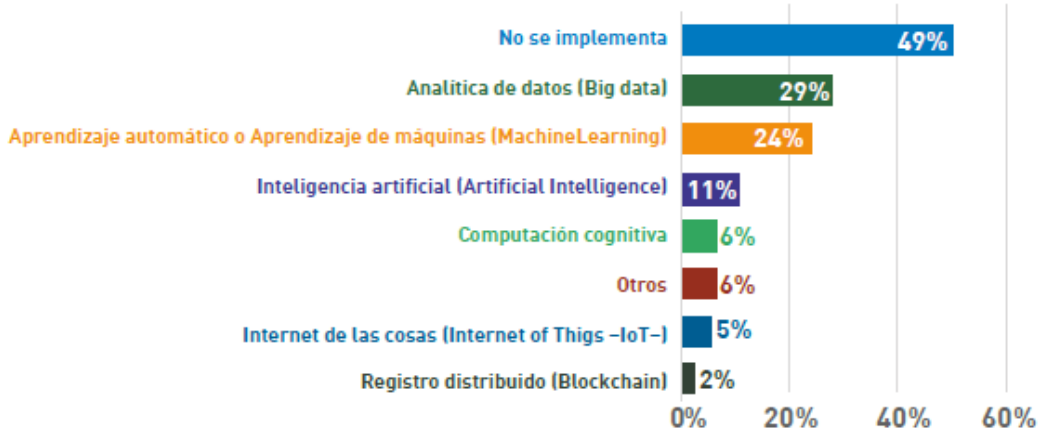


Nota: 191 registros

Fuente: *SG/OEA a partir de la información recolectada de entidades bancarias en América Latina y el Caribe*

El estudio también ha logrado evidenciar la brecha tecnológica en Latinoamérica respecto de las tecnologías digitales emergentes aplicadas a la gestión del riesgo de ciberseguridad. 49% de las organizaciones que participaron en el estudio no han implementado ninguna tecnología a pesar del crecimiento y evolución de las amenazas cibernéticas cada vez más automatizadas y frecuentes. Solo el 29% cuenta con procesos de analíticas de datos y 24% lo aprovecha con aprendizaje automático, a pesar del papel clave que estas capacidades tecnológicas representan en la prevención y detección de los ciberataques, ya sea contra los clientes o la infraestructura tecnológica de la organización (ver Gráfico 27).

Gráfico 27: Tecnologías digitales emergentes aplicadas a la seguridad digital



Nota: 187 registros

Fuente: *SG/OEA a partir de la información recolectada de entidades bancarias en América Latina y el Caribe*

Finalmente, respecto de las características de los incidentes de seguridad digital, se identificó que las mayores preocupaciones de las entidades bancarias son los riesgos por alteraciones de sitio web (*defacement*) y los sabotajes a través de personas enteradas (ver Gráfico 28). En relación con los eventos ya materializados, la infección de códigos maliciosos y *malware* son la modalidad con mayor incidencia tanto en bancos grandes como pequeños y medianos. Asimismo, se evidencia que la ingeniería social es uno de los orígenes que producen la vulneración de los controles de seguridad digital; esto refuerza la necesidad de capacitación y entrenamiento para generar conciencia sobre los riesgos de ciberseguridad en el personal de la empresa (ver Gráfico 29).

Gráfico 28: Riesgos cibernéticos que merecen mayor atención por parte de la entidad bancaria

	Grande	Mediano	Pequeño	Total
Robo de base de datos critica	2,87	2,83	2,83	**2,83**
Compromiso de credenciales de usuarios privilegiados	3,18	3,18	3,18	**3,18**
Pérdida de datos	3,57	3,61	3,57	**3,61**
Secuestro de información	3,77	3,70	3,73	**3,70**
Denegación del servicio	4,25	4,29	4,33	**4,29**
Sabotaje a través de un insider	4,80	4,82	4,78	**4,82**
Defacement – alteración en sitio web	5,56	5,57	5,58	**5,57**

Nota: 187 registros y los entrevistados priorizaban los riesgos del 1 al 7, siendo el 1 el riesgo más alto y 7 el riesgo más bajo.

Fuente: *SG/OEA a partir de la información recolectada de entidades bancarias en América Latina y el Caribe*

Gráfico 29: Eventos de seguridad digital contra las entidades bancarias grandes, identificados en los últimos doce meses

	Grandes			Medianas			Pequeñas		
	No hay	Si hay	Total	No hay	Si hay	Total	No hay	Si hay	Total
Ingeniería social	14%	86%	100%	40%	60%	100%	65%	35%	100%
Código malicioso o Malware	11%	89%	100%	14%	86%	100%	32%	68%	100%
Phishing dirigido para tener acceso a sistemas del banco	32%	68%	100%	34%	66%	100%	58%	42%	100%
Pérdida de datos	61%	39%	100%	68%	32%	100%	92%	8%	100%
Pérdida o robo de equipos o dispositivos	39%	61%	100%	49%	51%	100%	80%	20%	100%
Ataque de negación del servicio (DoS / DDoS)	43%	57%	100%	66%	34%	100%	80%	20%	100%
Robo de DNS	75%	25%	100%	89%	11%	100%	95%	5%	100%
Violación de políticas de escritorio limpio (Clear Desk)	14%	86%	100%	31%	69%	100%	55%	45%	100%
Sabotaje interno	71%	29%	100%	83%	17%	100%	91%	9%	100%
Fraude interno	21%	79%	100%	52%	48%	100%	85%	15%	100%
Defacement	75%	25%	100%	92%	8%	100%	97%	3%	100%
Backdoor (código desarrollado para habilitar acceso posterior)	50%	50%	100%	82%	18%	100%	94%	6%	100%
SQL Injection	36%	64%	100%	63%	38%	100%	83%	17%	100%
Ataque de fuerza bruta	46%	54%	100%	67%	33%	100%	82%	18%	100%

Fuente: *SG/OEA a partir de la información recolectada de entidades bancarias en América Latina y el Caribe*

Pensando hoy, mirando el mañana

El ecosistema digital se caracteriza por el cambio constante. Por este motivo es vital, para una organización que quiere triunfar en este entorno, mantener un monitoreo de las iniciativas de cambio digital (como las ya impulsadas por Google, Amazon, Facebook y Apple) a efecto de incorporar en los esquemas de seguridad y control estos nuevos enfoques, a la vez de determinar qué capacidades internas y externas se requieren para este fin. Asimismo, debe prestarse especial atención y cuidado a los riesgos vinculados a la transformación digital y desarrollos bajo esquemas de metodologías ágiles e impulsadas por enfoques de co-creación, interpretando adecuadamente la brecha generacional para la estrategia ante ataques cibernéticos.

Los desafíos que nos presenta el avance de la seguridad digital radican principalmente en contar con capacidades que permitan alinear el desarrollo tecnológico con las políticas existentes para la gestión de riesgos en ciberseguridad. Claramente en la región de Latinoamérica se tiene una brecha importante en este campo, tal como se evidencia en diversos estudios de organismos internacionales e incluso instituciones de los propios países que conforman la región.

Se sugiere invertir en conocimiento como real prevención, teniendo en cuenta que las nuevas tipologías del ciberdelito evolucionan con mayor celeridad que la legislación vigente. A medida que evoluciona la tecnología, también se desarrollan nuevas y sofisticadas amenazas cibernéticas. Debido a ello las organizaciones deben establecer un plan de manejo de crisis y construir capacidades de resiliencia que aborden los riesgos cibernéticos. Las organizaciones deben estar preparadas para dar respuestas rápidas a los ataques cibernéticos, permitiendo que los servicios que prestan no se vean interrumpidos; asimismo, fortaleciendo sus capacidades de identificación, contención, prevención, respuesta, recuperación y mejora continua contra las ciberamenazas. La construcción de un modelo de gestión de crisis ante ataques cibernéticos requiere la cooperación y compromiso de las distintas autoridades de las organizaciones e instituciones gubernamentales.

Para el diseño de un plan de respuesta ante ciberataques, es necesario conocer directamente las brechas de la organización, asumir que el ciberatacante las conoce, pensar que las personas se equivocan y que la tecnología en los planes podría ser obsoleta. Es necesario probar el plan de crisis de la manera más real, pensando que el ataque ocurrirá tarde o temprano. Es importante considerar la contratación de seguros especializados como transferencia de riesgos y la generación una buena red de contacto para capacidades externas a la que en algún momento se tendrá que recurrir.

La banca, independientemente de ser una industria amplia y detalladamente regulada, debe activar permanentemente su capacidad de autorregulación para enfrentar los riesgos cibernéticos y fijar estándares con permanente pauta de revisión ante los factores de escalabilidad, tecnología de última generación (robótica, inteligencia artificial) y constante evolución de las tipologías que los caracteriza. Es importante la oportuna adecuación del mapa de riesgos y estrategia de mitigación de las instituciones ante ciberamenazas automatizadas. Estos modelos de prevención requieren ser soportados por plataformas tecnológicas que interpreten en tiempo real y con alta capacidad predictiva; además, de lograr sinergias con las instituciones del estado a cargo de la ciberseguridad del país.

Se debe reconocer y considerar en el planeamiento la poca información que tiene el cliente interno/externo sobre los riesgos. Por este motivo es idóneo incorporar en las políticas nacionales de educación un currículo específico sobre ciberseguridad para la etapa escolar, a fin de disminuir la brecha existente del “analfabetismo digital”, que hoy es el principal riesgo del ciudadano común ante la ciberdelincuencia global.

Finalmente, a través del análisis realizado en este capítulo, se evidencia la brecha en la gestión de los riesgos de ciberseguridad en la región donde hay importantes oportunidades de mejora en los aspectos de aplicación de tecnología, capacitación y entrenamiento y regulación. La visión de los negocios está cambiando y el cierre de estas brechas permitirá acompañar la estrategia de transformación digital de la región en miras de su bancarización.

Tres años después de Bangladesh: Enfrentando a los Adversarios

SWIFT

Introducción

En febrero de 2016, Bangladesh Bank sufrió un ciberataque contra la infraestructura del banco que se encontraba conectada a SWIFT. Inmediatamente después del ataque, SWIFT lanzó su Programa de Seguridad del Cliente (CSP, por sus siglas en inglés), en una gestión concertada para incitar la colaboración en toda la industria contra la amenaza cibernética y ayudar a reforzar y salvaguardar la seguridad del ecosistema más generalizado.

Una inteligencia relevante y oportuna es un factor crítico para la defensa efectiva contra las amenazas cibernéticas. Es por eso que establecimos un equipo dedicado de Inteligencia de Seguridad del Cliente (CSI, por sus siglas en inglés) para investigar los incidentes de los clientes y para compartir información con la comunidad de manera anónima. Centrado en análisis y estudios forenses de seguridad del cliente, el equipo de CSI realiza investigaciones sobre posibles amenazas e incidentes de seguridad del cliente y comparte la información resultante con la comunidad a través del portal de intercambio de información SWIFT ISAC.

Tres años después de implementado el CSP, hemos publicado varias actualizaciones sobre cómo han progresado el modus operandi, las tácticas, técnicas y procedimientos (TTP, por sus siglas en inglés), entregando información valiosa sobre cómo deberían evolucionar las medidas de prevención y detección cibernética.

A principios de 2018, SWIFT se propuso aumentar su colaboración con expertos de la industria, incluidos los proveedores de antivirus y los equipos de respuesta a incidentes. Las gestiones dieron frutos rápidamente, ya que esa colaboración mucho más cercana culminó en una rápida identificación de las instituciones financieras atacadas por los ciberdelincuentes, en la mayoría de los casos incluso antes de que se enviaran unas transacciones fraudulentas.

La mayoría de estos ataques fueron identificados y detenidos en la fase de preparación. Sin embargo, en un grupo más reducido de esos intentos de ataque, los atacantes lograron emitir instrucciones de pago transfronterizas fraudulentas. Afortunadamente, muchas de estas instrucciones fraudulentas pudieron ser detenidas más tarde, gracias a la intervención de los bancos en la cadena de pago.

Si bien las medidas de detección de fraude y ciberseguridad son, ante todo, la responsabilidad del remitente, queda demostrado que las instituciones financieras involucradas en el flujo de pagos también pueden desempeñar funciones clave en la identificación y detección del fraude, funciones que se vuelven cada vez más importantes a medida que aumenta la velocidad de los pagos en efectivo, como está sucediendo. De hecho, aunque pasaron varios días no laborables entre el ataque y los pagos finales en el caso del Banco de Bangladesh, en los últimos casos los pagos en efectivo se han producido en cuestión de horas.

En este informe examinamos las tendencias que hemos observado en el transcurso de 2018 y 2019, mostrando cómo la información comercial y de seguridad puede utilizar señales reveladoras y volverse clave en la detección y respuesta a intentos de ataque.

A pesar de tener mayores éxitos en la detección y prevención de ataques, es de vital importancia que los participantes de la industria y sus socios en seguridad comprendan cómo han evolucionado los atacantes y cuán rápido pueden adaptar sus patrones de ataque para evitar la detección. Este informe, junto con los detalles técnicos publicados en el portal SWIFT ISAC, tiene como objetivo ayudar a los clientes en este esfuerzo.

Las características principales presentadas en este informe se relacionan con la evolución en la localización de los bancos objetivo, en los montos intentados en cada transacción fraudulenta, y en la oportunidad y las prácticas de reconocimiento de los atacantes. El informe también describe cómo los atacantes están variando sus prácticas en lo que respecta al momento adaecuado y las monedas preferidas, e identifica las ubicaciones regionales de las cuentas comprometidas o "mulas" utilizadas en estos intentos de robo.

Objetivos

SWIFT ha colaborado estrechamente con expertos de la industria, como proveedores de antivirus y equipos de respuesta a incidentes. Esta colaboración, que se intensificó considerablemente durante 2018, ha contribuido a la identificación proactiva de las instituciones financieras que son el blanco de los ciberdelincuentes.

En la mayoría de estos casos, los ataques han estado en la fase de reconocimiento; los atacantes han logrado comprometer las estaciones de trabajo de los usuarios, pero no han podido acceder a los sistemas de pago de los bancos.

Si bien SWIFT no revela los nombres de las instituciones financieras que han sido blanco de ataques cibernéticos, sí puede revelar información anónima relacionada con estas, como las características comunes que tienen las instituciones objetivo típicas, que otras entidades podrán usar preventivamente.

En la mayoría de los casos, los bancos objetivo se ubican en países con una calificación de (muy) alto riesgo en el Índice ALA de Basilea.[99] En el transcurso de los últimos quince meses, la mayoría de los ataques han sido dirigidos a instituciones financieras en África, Asia central, Asia oriental y sudoriental y América Latina.

En todos los casos, las instituciones objetivo eran bancos más pequeños en términos de transacciones transfronterizas por día.

Además de garantizar que los entornos estén protegidos desde un punto de vista técnico, todas las instituciones financieras deberían poder detectar transacciones fraudulentas y estar listas para responder a nivel comercial si descubren que son víctimas de ataques. Todos los clientes de SWIFT deben familiarizarse plenamente con el proceso y los mensajes de cancelación de pago, así como con el servicio de innovación de pagos globales (global payments innovation - gpi, por sus siglas en inglés) denominado de Detención y Recuperación (***gpi Stop and Recall facility***).

En la gran mayoría de los casos investigados, se insertaron transacciones fraudulentas utilizando la interfaz GUI. Esto significa que las instrucciones no habrían estado presentes en las aplicaciones de back office de pago y, por lo tanto, habrían sido detectables a través de la verificación de los mensajes de conciliación

de estado de cuenta al final del día/inicio del día que generalmente son enviados por los propietarios de Cuentas Nostro. Estos mensajes contienen descripciones generales de las actividades en la Cuenta Nostro en el día dado.

Además, las instituciones financieras pueden optar por utilizar la herramienta de **Informe de validación diaria** de SWIFT para detectar el uso de nuevos corredores y/o grandes desviaciones en los corredores existentes y el **Servicio de controles de pago de** SWIFT, que les permite a las instituciones financieras garantizar que ciertas combinaciones de montos, monedas, corredores o países requieran confirmación fuera de banda. Si bien el Servicio de controles de pago solo se lanzó recientemente, la reconciliación al final del día basada en la herramienta de Informe de validación diaria ya ha demostrado ser invaluable para ayudar a los clientes en la detección de intentos de fraude y así evitar posibles pérdidas.

Cantidades

En los últimos tres años, los sistemas antifraude de los clientes y otros sistemas de detección de anomalías han ayudado a frustrar a los atacantes en muchos casos. El ajuste de estos sistemas es imprescindible para su éxito.

El envío de instrucciones de pagos de alto valor fraudulentos puede generar grandes recompensas, pero cuanto mayor sea el valor de la instrucción, mayor será el riesgo de activar sistemas de detección de fraude. Desde el incidente cibernético en Bangladesh, las cantidades enviadas en transacciones fraudulentas individuales han evolucionado, lo que las hace más difíciles de detectar. Hasta principios de 2018, típicamente se veían montos por transacción de diez o de decenas de millones de dólares. Sin embargo, desde entonces, los atacantes han reducido significativamente el promedio de montos de transacción a entre 250 000 USD y 2 MUSD, presumiblemente para ayudar a evitar la detección.

Como se señaló anteriormente, las transacciones fraudulentas generalmente se emitían utilizando nuevos "corredores de pago".[100] En los casos en que se utilizaron corredores existentes, notamos grandes desviaciones en el valor. Por lo general, vimos que los montos por transacción enviados en los corredores existentes eran mucho mayores que los montos "promedio" enviados en los últimos 24 meses. Los bancos seleccionados pueden identificar tales anomalías utilizando la herramienta de Informe de validación diaria, mientras que los bancos receptores y los bancos beneficiarios pueden implementar algoritmos similares para identificar comportamientos sospechosos basados en patrones de tráfico históricos.
En cada uno de estos ataques que investigamos, la mayoría de las transacciones emitidas fueron manejadas por uno o dos bancos receptores y estaban destinadas al mismo país beneficiario. En las investigaciones más recientes, el número de transacciones fraudulentas emitidas promedió alrededor de diez por incidente, en un período de dos horas.

Los bancos emisores pueden identificar, marcar e investigar tales aumentos en el tráfico utilizando la herramienta de Informe de validación diaria, mientras que los bancos receptores y beneficiarios pueden implementar técnicas de detección basadas en aumentos repentinos en los mensajes, utilizando corredores particulares, o combinaciones particulares de bancos emisores y países beneficiarios.

Reconocimiento

Atraídos por la perspectiva de ingresos potencialmente lucrativos, los atacantes son persistentes. A menudo ingresarán en un objetivo y esperarán semanas o incluso meses antes de lanzar un ataque, aprovechando ese tiempo para aprender patrones y comportamientos y planear su fraude. Si bien operarán "en silencio" durante este tiempo de reconocimiento, es un período crítico durante el cual podrían ser detectados.

La respuesta inicial a un intruso detectado es de vital importancia, incluso si no hay evidencia visible de robo o intento de robo.

Sin un plan de respuesta a incidentes de seguridad cibernética operando, es casi imposible garantizar una respuesta inicial adecuada. Una respuesta inadecuada puede conducir a la pérdida de información de investigación valiosa y a la incapacidad posterior para determinar el alcance total de la violación (por ejemplo, una lista exhaustiva de todos los alojamientos comprometidos y las credenciales de usuario, todos los datos extraídos y cualquier *malware* implementado).

Además, mientras los actores no hayan sido erradicados por completo de los entornos comprometidos, siguen siendo un riesgo. Una vez que se dan cuenta de que han sido descubiertos, pueden cambiar rápidamente de táctica u optar por permanecer inactivos por un tiempo antes de renovar su ataque cuando el objetivo disfruta de una falsa sensación de seguridad.

Marco de controles de seguridad del cliente de SWIFT

La seguridad de nuestra comunidad requiere la participación de todos y comienza con la seguridad propia de cada organización. Para apoyar esto, en marzo de 2017 SWIFT publicó el Marco de controles de seguridad del cliente (CSCF, por sus siglas en inglés).

El CSCF es un conjunto de controles de seguridad, tanto obligatorios como de asesoramiento, que establecen una línea de base de seguridad para todos los usuarios de SWIFT.
Los controles fueron desarrollados en conjunto con expertos de la industria y diseñados para estar en línea con los estándares existentes de la industria de seguridad de la información: PCI-DSS, ISO 27002 y NIST. Verificar el cumplimiento de los controles es un paso esencial para que los clientes aseguren su infraestructura relacionada con SWIFT.

Como parte del proceso de Gestión de cambios para el CSCF, las actualizaciones de control generalmente se anuncian a mediados de año, con verificación y cumplimiento de los controles obligatorios de cualquier nueva versión requerida entre julio y diciembre del año siguiente. El objetivo es permitir un tiempo suficiente, hasta de 18 meses, para que los clientes puedan presupuestar, planificar e implementar las actualizaciones necesarias.

Oportunidad

La oportunidad lo es todo, incluso para determinar el éxito de un ciberataque. El siguiente gráfico ilustra el papel que juega el momento adecuado, mostrando las horas locales en que se enviaron transacciones fraudulentas.

Se pueden identificar dos patrones principales:

1. Los atacantes intentan enviar mensajes fuera del horario comercial o durante los días festivos para evitar que la institución objetivo los detecte; o

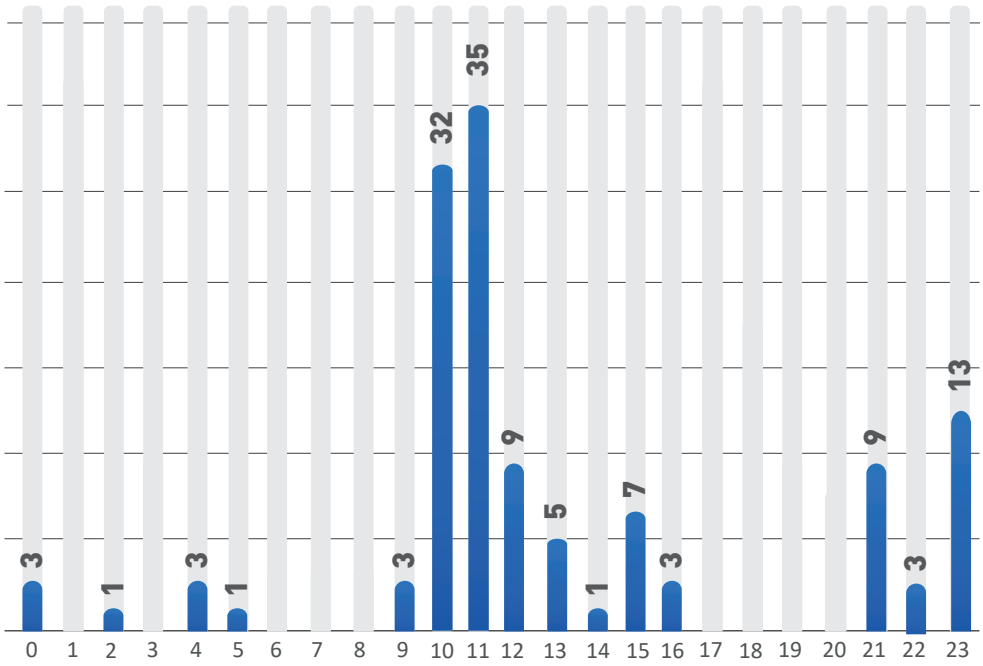
2. Los atacantes intentan enviar mensajes durante el horario comercial para semejarse al tráfico legítimo de la institución objetivo y pasar inadvertidos por la contraparte y las instituciones beneficiarias.

Los mensajes fraudulentos que no se detectan durante un período más largo de tiempo tienen una mayor probabilidad de llegar a las cuentas de Beneficiario y, como tal, tienen una mayor probabilidad de ser cobrados. La respuesta de manera oportuna a los incidentes de seguridad cibernética y contar con procesos de conciliación y cancelación estructurados y probados pueden ayudar a reducir el impacto financiero de un incidente de seguridad cibernética.

El ataque al Banco de Bangladesh tuvo lugar la noche previa a una serie de días no laborables en los diferentes países involucrados en los flujos de pago.

Sin embargo, en incidentes más recientes, los atacantes comenzaron a emitir pagos fraudulentos durante horas laborales en días hábiles. Además, en incidentes recientes, los retiros de dinero han ocurrido en cuestión de horas.

Gráfico 1: Numero de transacciones



Tipos de mensaje

Según los casos que hemos observado en los últimos 15 meses, el tipo de mensaje elegido por los atacantes en el fraude transfronterizo suele ser el tipo de mensaje de "Transferencia de crédito de cliente único" o MT103.[101] Además de algunos casos aislados, todas las transacciones fraudulentas emitidas durante incidentes cibernéticos de clientes conocidos por SWIFT se referían a mensajes MT103.[102]

Otra coincidencia notable es que todos los mensajes fueron procesados por al menos tres instituciones financieras diferentes en tres países diferentes:

1. El banco de destino ("BIC del remitente" o "Remitente")
2. El banco receptor o el propietario de la Cuenta Nostro del banco de destino ("BIC del receptor" o "Receptor")
3. El banco beneficiario ("Beneficiario" o "Cuenta en la institución")

Los tres bancos tienen papeles que desempeñar en la identificación de transacciones fraudulentas. En términos de SWIFT, se denomina la combinación de estos tres bancos el "corredor de pagos".

La gran mayoría de las transacciones fraudulentas que investigamos en los últimos 12 meses utilizaron corredores que no se habían utilizado en los 24 meses anteriores. Esto es especialmente interesante para

los bancos objetivo que pueden filtrar las transacciones salientes utilizando el Servicio de controles de pago de SWIFT para especificar qué corredores usan de manera regular, a la vez de requerir confirmación adicional en otros corredores.

Los bancos seleccionados también pueden identificar, marcar y hacer un seguimiento de nuevos corredores utilizando la herramienta de Informe de validación diaria de SWIFT, mientras que los propietarios de Cuentas Nostro pueden desempeñar un papel importante al identificar, marcar o consultar pagos a lo largo de nuevos corredores.

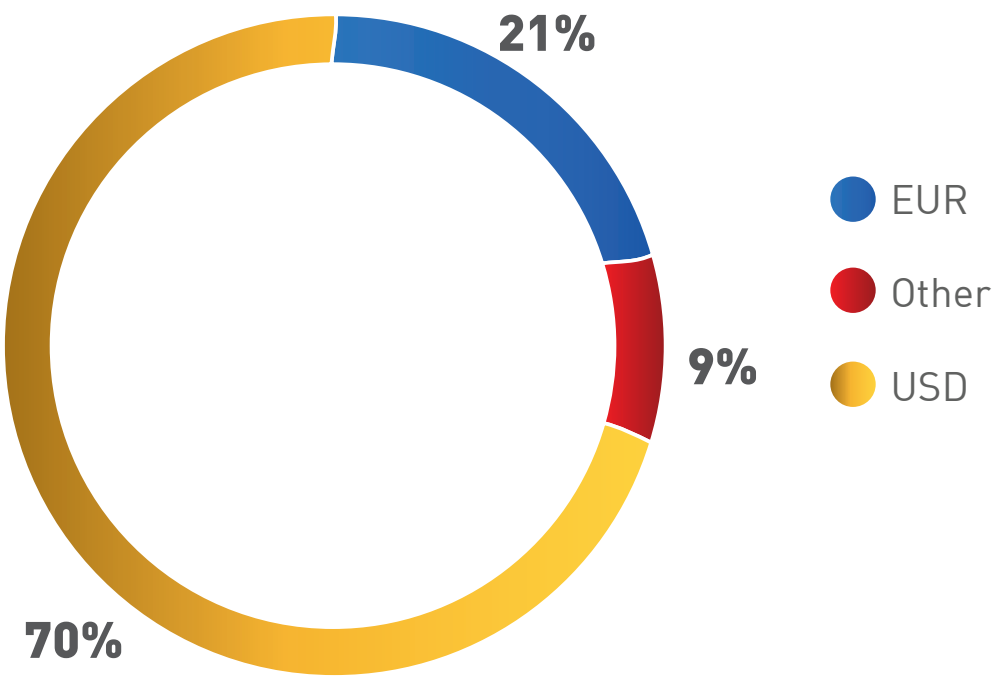
Monedas

Dado que el USD representa la mayor parte del tráfico transfronterizo, no sorprende que fuera la moneda utilizada en la mayoría de los incidentes investigados. En general, el USD representó aproximadamente el 70% de los mensajes fraudulentos creados desde el ataque de 2016.

Sin embargo, desde el incidente en Bangladesh Bank en 2016, también hemos observado un aumento en el uso de monedas europeas, especialmente EUR y GBP, mientras que una pequeña minoría de incidentes (aproximadamente 5%) se refirió a monedas de Asia Pacífico, principalmente HKD, AUD y JPY. Esto pone de manifiesto la importancia de que los bancos receptores presten atención al uso que hacen sus clientes de todas estas Cuentas Nostro internacionales, no solo cuentas en USD.

El siguiente gráfico muestra las monedas utilizadas en transacciones fraudulentas desde 2016.

Gráfico 2



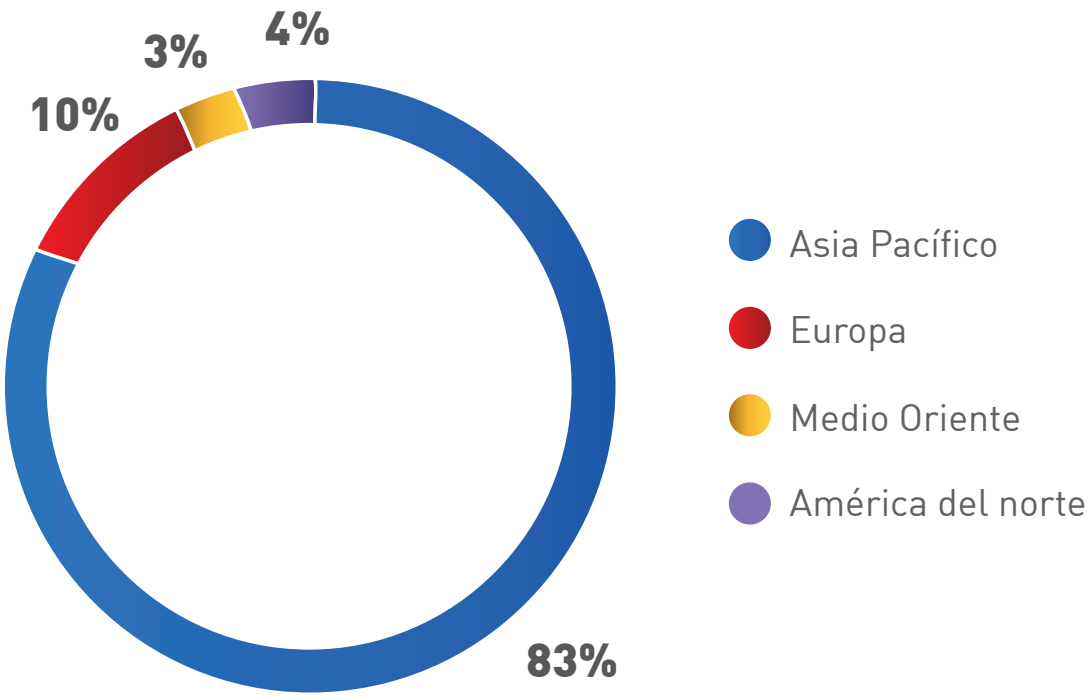
Beneficiarios

Las cuentas de beneficiario o "mulas" son críticas para que los atacantes puedan extraer fondos del sistema financiero; sin estas cuentas comprometidas, no podrían materializar ninguno de los fondos fraudulentos. Comprender el perfil de estas cuentas puede ser igualmente valioso para quienes luchan contra los fraudes.

El pequeño subconjunto de casos investigados en los que los adversarios lograron iniciar instrucciones de mensajes fraudulentos ofrece datos interesantes sobre las cuentas del Beneficiario. SWIFT pudo extraer información del país beneficiario de los mensajes fraudulentos enviados en 2018, información que reveló algunas diferencias en las técnicas de pago. Sin embargo, lo más notable fue la concentración de los bancos beneficiarios en Asia Pacífico: el 83% de todas las transacciones fraudulentas tenían una cuenta beneficiaria en Asia oriental y sudoriental. El 17% restante se extendió a otras regiones, incluyendo, en orden de magnitud, Europa, América del Norte y Medio Oriente.

El siguiente gráfico ilustra la ubicación regional de las cuentas de Beneficiario utilizadas en transacciones fraudulentas desde julio de 2018.

Gráfico 3



Fortalezca sus defensas

La herramienta de Informe de validación diaria y el Servicio de controles de pago son parte de la cartera de cumplimiento de delitos financieros de SWIFT y un elemento importante en el CSP para fortalecer las defensas de la comunidad financiera mundial contra las amenazas cibernéticas a medida que aumenta la frecuencia y la velocidad de los pagos.

Informe de validación diaria

La herramienta de Informe de validación diaria ayuda a mitigar el riesgo de pérdida de registros al proporcionar informes diarios de actividad y riesgo, de las transacciones SWIFT suyas del día anterior. El informe de actividad les permite a las instituciones verificar la actividad de sus mensajes de pago en el registro propio de SWIFT, lo cual es crítico si los entornos de los clientes se ven comprometidos. El informe de riesgos les permite a las instituciones centrarse en los cambios en la actividad que pueden indicar riesgos de pago significativos, proporciona totales de transacciones agregados por contraparte y señala nuevas relaciones de corresponsalía.

El informe de cada día cubre las actividades de pago del día anterior para los tipos de mensaje MT 103, MT 202, MT 202COV, MT 205 y MT 205COV. Los informes se entregan a través de un canal en línea completamente independiente y seguro, directo a los equipos de cumplimiento y operaciones para el monitoreo.

Servicio de controles de pago

El Servicio de controles de pago les permite a los clientes examinar las instrucciones de pago de forma segura, antes de la transmisión, para detectar cualquier flujo de mensajes ilícitos o inusuales.

Usando la herramienta, los clientes pueden definir su propia política de monitoreo, controlando sus parámetros para permitir la detección oportuna y la prevención de solicitudes de transferencia que no están dentro de la política o que son poco características y, por lo tanto, potencialmente de alto riesgo.

Al comprender los patrones de pagos enviados con el paso del tiempo, el Servicio de Controles de Pago les permite a los bancos implementar controles más efectivos y sólidos. Las reglas de monitoreo también se pueden implementar en tiempo real para hacer cumplir las políticas y proteger las operaciones de pago. Hacer esto reduce el riesgo de fraude y les brinda a los equipos de operaciones un control general más estricto.

Gestión de riesgos de la contraparte de ciberseguridad

Para que los clientes puedan certificar su nivel de cumplimiento de los controles obligatorios y de asesoramiento, SWIFT proporciona la herramienta de "Conozca a su cliente: certificación de seguridad" como la aplicación central para el envío de datos de autocertificación. La aplicación KYC-SA también le permite a cada cliente facilitar el intercambio transparente de su información de estado de seguridad con sus contrapartes para apoyar la gestión de riesgos cibernéticos y la debida diligencia comercial.

La transparencia que brinda este sistema de intercambio de datos con contrapartes está impulsando la certificación y el cumplimiento de los controles, ya que las instituciones buscan demostrar su seguridad cibernética a sus contrapartes.

El riesgo de seguridad cibernética introducido por las contrapartes debe gestionarse junto con otros tipos de riesgo. Por lo tanto, muchas instituciones ya están integrando evaluaciones de riesgo cibernético en sus procesos de riesgo existentes, al incorporar la evaluación de los datos de certificación CSCF de las contrapartes en sus procesos de gestión de riesgos y toma de decisiones comerciales.

Como se describe en la guía recientemente publicada "Evaluación del riesgo de las contrapartes de seguridad cibernética: una guía de inicio", las instituciones pueden evaluar el riesgo de seguridad cibernética que plantean sus contrapartes, mediante:

- La recopilación de los datos necesarios y la correlación de incidentes conocidos para respaldar las decisiones basadas en riesgos;

- El procesamiento de estos datos y su transformación en una evaluación ponderada basada en el riesgo, que generalmente se muestra como una puntuación numérica o un indicador rojo-ámbar-verde;

- La adopción de contramedidas adecuadas para mitigar o "tratar" los riesgos;

Para respaldar la evaluación del riesgo de las transacciones entrantes de las contrapartes, las instituciones deben evaluar cómo se correlacionan las transacciones entrantes de las contrapartes con el perfil de incidentes existentes, por ejemplo: país/región de la contraparte emisora; país/región del beneficiario final; tipo de transacción; moneda de transacción; valor de la transacción; tiempo de la transacción y frecuencia.

Estos parámetros se describen en la Guía de inicio y deben ser utilizados por las instituciones para evaluar los niveles de riesgo de las contrapartes.

Conclusión

La comunidad financiera mundial ha visto una evolución continua en la amenaza cibernética desde 2016, en la que instituciones financieras están sufriendo ataques con niveles crecientes de sofisticación.

Para responder a este desafío, SWIFT continuará promoviendo estándares sólidos de seguridad cibernética, buscará innovaciones que mejoren la seguridad en nuestros propios productos y servicios, y velará por aumentar el alcance y la calidad del intercambio de inteligencia sobre amenazas.

Nuestra iniciativa de intercambio de información ha contribuido a tener mejoras significativas en las defensas cibernéticas colectivas de la comunidad, así como a la introducción de capacidades de detección y prevención de fraude, como el Servicio de controles de pago y la herramienta de Informe de validación diaria.

Estos productos están destinados a mitigar los riesgos asociados con el fraude cibernético y están diseñados para complementar los controles de fraude que las instituciones financieras ya deberían tener.

La industria debe aumentar continuamente la fuerza y la diversidad de sus defensas y asegurarse de que comprende la naturaleza de la amenaza cambiante. Esto significa ser proactivo en limitar las oportunidades criminales relacionadas con los sistemas y las prácticas comerciales, y garantizar la preparación adecuada y comprender el riesgo cibernético de la contraparte.

COLOMBIA

Ciberseguridad: una oportunidad de crecimiento que nos desafía hacia una adecuada gestión del riesgo

Jorge Castaño

El crecimiento acelerado de tecnologías innovadoras, el aumento de la conectividad y la adaptación a estas traen consigo ventajas innegables desde la perspectiva económica de los Estados. Vivimos una realidad que implica que cada día más poblaciones adoptan el uso de internet, y, a su vez, los distintos sectores de la economía aprovechan las ventajas de las nuevas tecnologías para innovar, diversificar sus negocios, generar valor, ser más competitivos, mejorar la experiencia del cliente y beneficiarse a gran escala mediante la implementación de procesos colmados de mayor eficiencia e inclusión.

La adopción de estos desarrollos recientes envuelve la exposición a nuevos riesgos. La cotidianidad acompañada del uso de tecnologías inclina la atención hacia la necesidad de gestionar asuntos relativos al control de acceso a las redes, la identificación de vulnerabilidades, la prevención de fugas de información y de fraudes, así como la atención de eventuales incidentes de seguridad. Lo anterior se convierte en una consecuencia natural de trasladar las actividades del mundo físico al digital apoyados en estas nuevas herramientas, las cuales, a su vez, incrementan los puntos de posibles vulnerabilidades.

El principal desafío de esta transformación es desarrollar la capacidad para contrarrestar las contingencias de la implementación de tecnologías innovadoras. Se vuelve imperativo gestionar y reducir las deficiencias o debilidades de los sistemas de información para evitar que actores ilegales generen pérdidas financieras a las empresas, sustraigan información confidencial, causen interrupción del negocio o afecten la reputación de las organizaciones. Por esta razón la ciberseguridad reviste una enorme importancia para los gobiernos —a nivel individual y global— y para las sociedades que cada vez evolucionan de forma interconectada.

El sistema financiero no ha sido ajeno a los desarrollos tecnológicos. Su adopción ha significado profundos cambios en la concepción de la prestación de los servicios financieros y, por supuesto, ha acentuado la necesidad de reevaluar la gestión adecuada de los riesgos inherentes a estas actividades, los cuales no son menores. De acuerdo con la información publicada por la Organización de los Estados Americanos (OEA) en el documento *Estado de la ciberseguridad en el sector bancario en América Latina y el Caribe*[103] (2018), nueve de cada diez bancos de América Latina y el Caribe sufrieron incidentes cibernéticos durante el último año y el 37% de los bancos de la región fueron víctima de ataques que resultaron efectivos. Indica además que seis de cada diez usuarios que no utilizan servicios de banca digital lo hacen por desconfianza de la seguridad de las transacciones.

De otro lado, de acuerdo con las cifras publicadas por el Centro Cibernético Policial, durante el 2018 en Colombia se registraron 21.687 denuncias por delitos informáticos, lo que representa un incremento del 36% en el número de casos respecto al 2017, cuando se denunciaron 15.942 casos, según fuentes de la Fiscalía General de la Nación. El hurto por medios informáticos fue el delito de mayor afectación en 2018

con 12.014 denuncias y el 55% de los casos de cibercrimen está asociado a afectación patrimonial de los colombianos por ataques a sus cuentas bancarias.

De allí la importancia de consolidar la confianza en un sector financiero que se adentra en un ecosistema digital, promueve la reducción del uso de efectivo, la utilización de nuevas tecnologías y promueve la inclusión. Para este propósito es fundamental propender por un entorno seguro que garantice el funcionamiento adecuado del sector al tiempo que protege y garantiza los derechos de los usuarios.

La importancia de la gestión del riesgo de ciberseguridad se acentúa por el potencial que tiene de trascender y ser sistémico. Por esta razón, varias organizaciones internacionales se han enfocado en el análisis y establecimiento de un marco conceptual de los riesgos asociados al uso de nuevas tecnologías. El Consejo de Estabilidad Financiera[104] (FSB, por sus siglas en inglés) definió el riesgo cibernético como aquel que implica una pérdida financiera o afectación a la reputación de una organización, derivado de una falla en sus sistemas tecnológicos de información. Por su parte, el Fondo Monetario Internacional[105] (FMI) definió aspectos relacionados con los costos asociados a los ataques cibernéticos, señalando que existen costos directos relacionados con aquellos gastos en los que se debe incurrir para el cubrimiento de investigaciones forenses, asesorías legales, protección y seguridad del cliente, entre otros; e indirectos, que comprenden aquellos que tienen menor visibilidad y efectos a largo plazo.

En el contexto regional el análisis y estudio de estos asuntos no ha tenido menor relevancia. De acuerdo con el informe Ciberseguridad. *¿Estamos preparados en América Latina y El Caribe?*[106], publicado por el Banco Interamericano de Desarrollo (BID) y la OEA (2016), Latinoamérica es una región que cuenta con el cuarto mayor mercado móvil del mundo y se encuentra en un proceso de adaptación de medios digitales en el relacionamiento de los gobiernos con sus ciudadanos. Así mismo, considera que "una enorme mayoría de nuestros países aún están poco preparados para contrarrestar la amenaza del cibercrimen", y "muchos países de la región son vulnerables a ataques cibernéticos potencialmente devastadores". Estas afirmaciones las sustenta en la existencia de debilidades asociadas a circunstancias como la falta de estrategias de ciberseguridad y planes de protección de infraestructura crítica y la falta de capacidad para perseguir estos delitos.

De acuerdo con la visión general del estado de la seguridad cibernética en Colombia, para ese momento[107] el país cuenta con una estrategia de seguridad cibernética nacional y un programa de seguridad cibernética coordinado vinculados a los riesgos, prioridades y objetivos nacionales. Así mismo, asegura que se han identificado amenazas específicas a la seguridad nacional en el ciberespacio, pero aún no se cuenta con una estrategia de respuesta coherente.

En materia de coordinación destaca que existen acuerdos entre los sectores público y privado en materia de defensa cibernética y que agencias líderes del Estado, así como empresas líderes del sector privado han comenzado a darle prioridad a la seguridad cibernética mediante la identificación de riesgos, amenazas y prácticas de alto riesgo.

Con respecto a temas sociales, considera que se ha desarrollado una conciencia social del uso seguro de los sistemas en línea y que existen programas sobre la concientización sobre la importancia de la seguridad cibernética. Se han implementado esfuerzos para proporcionar servicios en línea más seguros con asignaciones presupuestales mínimas y los servicios de comercio electrónico son pocos y no totalmente organizados.

Acerca de los marcos regulatorios de seguridad cibernética destaca que se está adelantando la estructuración de marcos legales relacionados con el tema y resalta la importancia de que exista

normatividad en materia de protección de datos de los individuos y tipificación de delitos informáticos. Sin embargo, llama la atención respecto de la limitada capacidad institucional para la construcción de casos basados en información electrónica.

Frente a estas conclusiones es importante señalar que desde hace varios años el Gobierno colombiano ha implementado como política pública el fortalecimiento de la conectividad, el acceso a nuevas tecnologías, internet y el uso de plataformas digitales que permitan acercar regiones del país tradicionalmente apartadas (Conpes 3072-3670).

Así mismo, consiente de los nuevos desafíos del uso del entorno digital, ha establecido la Política Nacional de Seguridad Digital (Conpes 3854[108]), la cual se ha enfocado en incluir como parte de la Política de Ciberseguridad y Ciberdefensa definida en el documento Conpes 3071 la gestión del riesgo en el entorno digital, fortaleciendo así el esquema gubernamental para contrarrestar las amenazas cibernéticas que emergen como respuesta a la incorporación de las nuevas tecnologías en el desarrollo de actividades económicas y sociales del país.

En ese documento se plantea "la importancia del entorno digital como herramienta para el crecimiento económico, las nuevas y más sofisticadas formas para atentar contra la defensa y seguridad de los ciudadanos y la del Estado, la diversidad de afectados por los incidentes digitales en el país, y la concentración de los mismos en la ciudadanía, resaltan la importancia de que el país tenga un enfoque de gestión de riesgos en seguridad digital (...)". Con este propósito, el estudio lista los principales problemas que se advierten para lograr este objetivo, entre los cuales vale la pena destacar la falta de una visión estratégica en seguridad digital basada en riesgos, la necesidad de maximizar las oportunidades que tienen las múltiples partes interesadas en el entorno digital[109], el apremio por desarrollar capacidades de ciberseguridad y ciberdefensa y fortalecer la cooperación nacional e internacional en materia de seguridad digital.

A partir del diagnóstico de cada uno de estos desafíos se define la Política Nacional de Seguridad Digital, la cual busca fortalecer las capacidades de las partes interesadas para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades, apoyados en la cooperación, colaboración y asistencia (Conpes 3854); establece objetivos estratégicos y estrategias para el logro y ejecución de los mismos, los cuales comprenden la creación de un marco institucional con un enfoque en la gestión de riesgo, el fortalecimiento de un ecosistema digital seguro, la construcción de confianza en el entorno digital y la promoción de esquemas de protección basados en mecanismos permanentes y estratégicos para impulsar la cooperación a nivel nacional e internacional.

En este punto es necesario señalar los recientes avances que en materia regulatoria ha materializado el gobierno. El 24 de junio de 2018 se promulgó la Ley 1928 de 2018 "por medio de la cual se aprueba el 'Convenio sobre ciberdelincuencia', adoptado el 23 de noviembre de 2001 en Budapest, instrumento que impulsa la colaboración, cooperación y asistencia en la lucha contra el delito cibernético y supone la adaptación de un arreglo institucional que involucra un catálogo de figuras dedicadas a penalizar las modalidades de criminalidad informática[110], el establecimiento de normas de carácter procesal que promuevan salvaguardar la evidencia digital (reglas para la obtención y conservación de datos digitales que sirvan como pruebas) y la promoción de la cooperación internacional como herramienta para investigar cualquier delito que involucre evidencia digital, ya sean delitos tradicionales o informáticos. La adhesión al convenio sin duda aporta herramientas y procedimientos para seguir luchando contra el cibercrimen y fortalece las políticas públicas en esta materia. Estamos a la espera del examen automático de constitucionalidad para su implementación.

En esta misma línea, es importante destacar que en 2017, producto de la colaboración de la OEA, el Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia (MinTic) y el BID, se publicó un informe sobre impactos en Colombia de los incidentes de seguridad digital. Dentro de las principales conclusiones de este trabajo se encuentra una percepción, por parte de las entidades públicas y privadas participantes, de contar con mecanismos suficientes e idóneos para responder a eventos que comprometan aspectos de seguridad digital como un ataque cibernético. Así mismo, se destacaron aspectos de especial atención, como la insuficiencia de recursos que presentan algunas organizaciones para asegurarse contra los incidentes digitales, la necesidad de que las entidades públicas de orden territorial adopten más medidas de seguridad, la importancia de contar con áreas de dedicación exclusiva para la atención de incidentes de esta naturaleza y la importancia de empezar a estimar los costos que estos riesgos implican para las organizaciones.

Como se mencionó, el desarrollo de herramientas digitales en los diferentes sectores de la economía ha tenido un incremento exponencial en los últimos años. El sistema financiero no ha sido ajeno a este fenómeno, lo cual ha redundado en beneficio del consumidor financiero y de las propias entidades. Esta oportunidad para el desarrollo del sector y de la inclusión en el mismo supone, a su vez, retos desde el punto de vista del regulador y del supervisor financiero.

Conscientes de esta realidad, en 2017 el supervisor financiero colombiano estableció como prioridad de supervisión la necesidad de efectuar un análisis de la gestión del riesgo de ciberseguridad dentro de sus entidades vigiladas y realizó un diagnóstico respecto de la capacidad de reacción de estas a un evento de vulnerabilidad en materia de seguridad digital. La metodología del diagnóstico consistió en realizar una encuesta a 59 entidades supervisadas por la Superintendencia Financiera de Colombia (SFC), la cual contenía preguntas destinadas a establecer el estado de madurez de la gestión del riesgo de ciberseguridad.

Dentro de las principales conclusiones arrojadas por este trabajo se encontró que las entidades encuestadas reciben anualmente cerca de 40 millones de ataques cibernéticos. Tal exposición existe en un contexto en el que el 93% de las entidades utiliza estándares internacionales para la gestión de la seguridad de la información, el 100% cuenta con comités para discutir temas de seguridad de la información y de seguridad digital, el 83% ha definido planes para fortalecer la gestión de la seguridad de la información y el 76% de las entidades cuenta con estrategias de comunicación y alianzas con organismos de defensa para brindar mayor solidez a sus esquemas de protección.

De acuerdo con los datos arrojados, las inversiones destinadas a la tecnología y la gestión de la seguridad de la información van en aumento. Las entidades realizan, anualmente, análisis de vulnerabilidades a las redes y sistemas de información, un alto porcentaje de las encuestadas (86%) realizan al menos una vez al año pruebas o simulacros de atención de crisis y recuperación de incidentes de seguridad, se cuenta con centros de operación de seguridad que monitorean, en tiempo real, la actividad de los sistemas informáticos internos con el propósito de prevenir incidentes de seguridad y de responder rápidamente en caso de que ellos ocurran.

En este mismo sentido, se estableció que más del 50% de las entidades cuenta con soluciones SIEM (Security Information Event Management) que permiten recopilar registros e información relacionada con la seguridad informática, analizarla, detectar posibles comportamientos anómalos y tomar medidas defensivas oportunas, y realizan dos o más veces al año pruebas de hacking ético para encontrar vulnerabilidades que pudieran facilitar la intrusión de ciberdelincuentes a los sistemas de información.

Los datos referenciados mostraron que las entidades financieras en Colombia tienen conciencia de los riesgos de seguridad que comportan el uso de nuevas tecnologías y que han adoptado medidas tendientes a evitar y administrar eso riesgos de manera que no identificaron ataques con la potencialidad de afectar la prestación de sus servicios o la seguridad de la información. Un aspecto para destacar es la evidencia de que los asuntos relacionados con seguridad de la información son abordados por altos directivos de las entidades, lo cual refleja el compromiso institucional con estas políticas.

En definitiva, se identificó que las entidades implementaron mecanismos de defensa idóneos para protegerse frente a los ataques cibernéticos y que sus análisis de vulnerabilidad les permiten identificar y corregir brechas de seguridad que podrían ser utilizadas para afectar la confidencialidad, integridad o disponibilidad de la información. A pesar del entorno positivo descrito en el sector financiero colombiano en materia de prevención y gestión de la ciberseguridad, las tendencias actuales harán más frecuentes, persistentes e indetectables los ataques cibernéticos. Esas tendencias se ven reflejadas en el sinnúmero de instrumentos digitales y tecnológicos que caracterizan el sistema financiero en la actualidad, que lo interconectan y evolucionan de manera constante.

Desde hace varios años, el sistema financiero colombiano ha ampliado su portafolio de canales transaccionales y de disponibilidad en diferentes medios tecnológicos. Sin embargo, además de ese acercamiento de los productos financieros al consumidor financiero, las entidades financieras en el mundo –tendencia que se verá replicada en Colombia– han empezado a implementar herramientas valiosas para el procesamiento de la información.

Así por ejemplo, hacen parte de esta tendencia la cadena de bloques (*blockchain*) para el registro y aseguramiento de las transacciones; herramientas de grandes datos (*big data*) y analítica de datos (*data analytics*) para el almacenamiento de grandes volúmenes de información y la toma de decisiones; aprendizaje automático (*machine learning*) para el otorgamiento de créditos, reconocimiento de siniestros y prevención del fraude; trading algorítmico (*algorithmic trading*) para la compra y venta de valores en los mercados electrónicos; computación en la nube (*cloud computing*) para el desarrollo, pruebas y operación de aplicaciones administrativas y misionales; inteligencia artificial (*artificial intelligence*) para manejar portafolios financieros; biometría (*biometrics*) para el reconocimiento y autenticación de los clientes; *IoT* o internet de las cosas para lograr una tarifación adecuada de las pólizas de seguros; smart contracts o contratos inteligentes en operaciones de comercio electrónico; las interfaces de programación de aplicaciones (API, por sus siglas en inglés) y servicios web (*web services*) para proveer información a otras organizaciones sin depender de elementos computacionales particulares.

Todas estas tendencias implican un uso intensivo de la información, de la mano de elevados niveles de interconectividad, lo cual comporta un incremento en la exposición de las entidades a los riesgos cibernéticos que deben ser identificados y gestionados. Estos riesgos, se avizoran en múltiples frentes. Por ejemplo, en materia de seguridad de la información, en particular, la que se almacena o procesa en medios electrónicos; el sector financiero se encuentra expuesto a las amenazas cibernéticas dada la naturaleza global de internet y de los sistemas de información en la industria que trascienden fronteras.

A nivel regional es conocido que el sistema financiero mexicano fue vulnerado en 2018, en particular en la operación del Sistema de Pagos Electrónicos Interbancarios (SPEI). Según el Banco de México, el 17 de abril del año pasado se registró la vulneración de un participante en el SPEI derivada de ataques cibernéticos. A partir de esa fecha se identificaron cuatro eventos adicionales: dos el 24 de abril, uno el 26 de abril y uno más el 8 de mayo. Estos ataques cibernéticos representaron en su momento montos involucrados de aproximadamente 300 millones de pesos mexicanos[111]. Estos eventos nos invitan a reflexionar en que el enfoque de la prevención de los riesgos en materia de ciberseguridad podría tener

un alcance regional en la medida en que los sistemas financieros están altamente interconectados y que las estructuras que buscan vulnerar los sistemas de informática de las entidades financieras trascienden fronteras con facilidad.

Una prevención efectiva debe abordar el problema de manera transversal, permitiendo a los organismos de supervisión nutrirse de la experiencia de sus pares en otras latitudes. La SFC registra de forma positiva las iniciativas de la OEA para el desarrollo de herramientas que permitan analizar y mejorar las capacidades en materia de ciberseguridad, tendientes a materializar el derecho de los consumidores a unos servicios financieros seguros.

En línea con estos nuevos y grandes desafíos, y con el fin de garantizar la adecuada gestión de estos riesgos por parte de las entidades financieras, el 5 de junio de 2018 la SFC expidió la Circular Externa 007[112] mediante la cual impartió instrucciones relacionadas con los requerimientos mínimos para la gestión del riesgo de ciberseguridad. Estos lineamientos responden a la creciente masificación del uso de canales digitales en la prestación de servicios financieros y surgen como complemento de los ya desarrollados y adaptados a los sistemas de administración de riesgos operativos y de seguridad de la información.

El propósito de esta normativa fue dar un trato específico al riesgo cibernético al que están expuestas las entidades mediante el establecimiento de un marco conceptual que facilita el entendimiento y la comprensión de los conceptos asociados a este, así como la construcción de unos principios y lineamientos que se deben cumplir para una adecuada gestión de las amenazas que comporta. Se definieron también algunas herramientas básicas que permiten reconocer la importancia y las particularidades de este riesgo y promover procesos generales de gestión.

Por ejemplo, se estableció la necesidad de que dentro de las entidades se cuenten con políticas, procedimientos, recursos técnicos y humanos para que la gestión de riesgo sea efectiva. Con ese propósito se establece un catálogo de medidas que implican responsabilidades de Gobierno Corporativo (aprobación de políticas en la materia por parte de la junta directiva), modificaciones a las estructuras organizacionales con la asignación de funciones específicas para el adecuado análisis, monitoreo y verificación de este tipo de amenazas (creación de unidades de gestión de riesgo de seguridad de la información y de ciberseguridad), la adopción de estándares internacionales en materia de sistemas para la gestión para la ciberseguridad tales como ISO 27032, NIST, el Foro en Seguridad de la Información (ISF, por sus siglas en inglés) y los controles críticos de seguridad (CSI, por sus siglas en inglés) y el cumplimiento de un conjunto de etapas que incluyen la prevención, detección, respuesta y recuperación a incidentes de seguridad de la información y de ciberseguridad.

Cada una de estas fases considera aspectos específicos, como la realización de pruebas de seguridad, continuidad del negocio, educación financiera a los consumidores, protocolos de colaboración con autoridades que hacen parte del modelo nacional de gestión de ciberseguridad, monitoreo continuo a las plataformas tecnológicas y la creación de procedimientos de respuesta a incidentes tales como desconexión automática de equipos, cambio de contraseñas y bloqueo de direcciones IP, entre otros. Resulta importante mencionar que la implementación de las instrucciones debe atender en todos los casos aspectos como la estructura de cada entidad, su línea de negocio, tamaño, canales de atención, número de clientes y servicios prestados, temas que determinan la evaluación de riesgo que sobre este tipo de elementos deben realizar y cuya adecuada ejecución exige un serio compromiso por parte de los actores involucrados.

Adicionalmente, es necesario abordar algunos asuntos respecto de la innovación tecnológica en servicios financieros (*fintech*), la cual se está desarrollando rápidamente fomentando transformaciones radicales

y trayendo consigo oportunidades y riesgos al sistema financiero, dentro de los cuales está el riesgo de ciberseguridad. Este asunto es particularmente importante en la medida en que muchas innovaciones no han sido probadas a través de un ciclo financiero completo y las decisiones tomadas en etapas tempranas pueden sentar precedentes importantes.

La rápida propagación de los ciberataques a gran escala en forma de servicio distribuido, el robo de datos, la pérdida de propiedad intelectual y el fraude cibernético existen desde hace más 15 años. No obstante, lo que marca hoy la gran diferencia es la velocidad con la que aumentan la frecuencia y el impacto de estos incidentes vs. la capacidad de las partes interesadas en reaccionar frente a cada uno de ellos.

Por esta razón, el Comité de Supervisión Bancaria de Basilea (BCBS, por sus siglas en inglés) y el Fondo Monetario Internacional (FMI)[113], entre otras organizaciones, han definido la urgencia de coordinar los esfuerzos internacionales para reforzar la resiliencia a ataques cibernéticos, es decir, la capacidad para recuperar el estado inicial del servicio cuando ha cesado la perturbación derivada de un incidente. Como se ha mencionado, durante los últimos años la regulación y la supervisión al riesgo cibernético se han convertido en una prioridad para los principales reguladores a nivel global. Los principales gobernadores de bancos centrales del G20 mediante el BCBS han abordado las preocupaciones en materia de ciberseguridad y resiliencia operacional con el objetivo de evaluar las medidas que garanticen el futuro de la regulación y supervisión financiera en estos aspectos[114]. La principal hipótesis es que *"el uso malicioso de las tecnologías de la información y la comunicación (TIC) podría perturbar servicios financieros cruciales para los sistemas financieros tanto nacionales como internacionales, menoscabar la seguridad y la confianza y poner en peligro la estabilidad financiera"*[115], lo cual hace urgente abordar respuestas que garanticen la resiliencia operacional y que van más allá de la gestión propia del riesgo operacional y los requerimientos mínimos de capital. Surge entonces el Grupo de Trabajo de Resiliencia Operacional (ORG, por sus siglas en inglés), cuyo propósito es identificar las prácticas vigentes, así como evaluar las deficiencias y las medidas de política que podrían mejorar la resiliencia operacional y, entre otras, contribuir a los esfuerzos internacionales relacionados con la gestión del riesgo cibernético.

Por otra parte, y a una escala sistémica, el FMI[116] ha identificado a los ataques cibernéticos como un riesgo para la estabilidad financiera en varios de sus informes sobre la estabilidad financiera mundial, toda vez que la experiencia reciente indica que este riesgo es dinámico y cambiante, flexible con la evolución tecnológica y particularmente adaptable a cambios en la regulación y supervisión. Estas características hacen que la regulación y la supervisión del riesgo cibernético sean labores especialmente complejas que requieren herramientas, personal especializado y marcos analíticos especiales.

Adicionalmente, en estos informes se resaltan varios de los posibles canales de transmisión identificados. Entre los más citados son las interconexiones financieras, las dependencias operacionales y los efectos sobre la confianza, aunque tanto las instituciones financieras como el sector oficial tienen dificultades para encontrar un conjunto de parámetros significativos y comparables para cuantificar y vigilar el ciberriesgo y valorar los niveles de resiliencia cibernética de las empresas.

El FSB publicó en octubre de 2017[117] un repaso de la regulación, las directrices y las prácticas de supervisión en materia de ciberseguridad publicadas a escala tanto nacional como internacional. Ejercicio que permitió constatar que la banca es el único sector de servicios financieros para el que todas las jurisdicciones pertenecientes al FSB han publicado como mínimo una regulación, directriz o práctica supervisora. Ante esta coyuntura, desde hace menos de un año, la ciberseguridad alcanzó el primer puesto de la lista de prioridades de los reguladores internacionales y, desde entonces, es el centro de atención de la mayoría de los organismos internacionales.

El Banco Central Europeo (BCE) y la Autoridad Bancaria Europea (ABE)[118] consideran prioritario crear barreras para combatir los ciberataques en la banca. Para 2019, la supervisión bancaria del Banco Central Europeo continuará evaluando los riesgos tecnológico y cibernético que afrontan las entidades e iniciará una serie de inspecciones in situ sobre cuestiones relacionadas con el riesgo tecnológico. Además, pedirá auditorías internas para comprobar el grado de seguridad y exigirá a las entidades significativas que continúen informando al BCE sobre cualquier ciberincidente importante que ayude a preservar la gestión.

Las *fintech* y la seguridad cibernética son temas importantes para los supervisores en América Latina. La Asociación de Supervisores Bancarios de las Américas[119] (ASBA), publicó un informe que detalla las expectativas de regulación y supervisión, en el que se evidencia que las nuevas tecnologías y sus riesgos ocupan los primeros lugares en el orden de eventos relevantes. Cinco de los principales temas de discusión están relacionados con regulación de fintech, riesgos tecnológicos y ciberseguridad y el desarrollo de las fintech y su asimilación en los mercados. Algunos de los productos y servicios fintech más prominentes en la región son la banca móvil, las plataformas digitales para el comercio, los mercados de divisas al mayoreo, las transferencias P2P y los mercados de préstamos. Pese a que en la región la presencia de estos productos y servicios es muy heterogénea, los miembros de esta asociación coinciden en que es un tema relevante en el que la transferencia de experiencias entre los principales reguladores y supervisores de la región permitirá avanzar hacia nuevas estrategias de supervisión.

En Colombia, la gestión de ciberseguridad constituye un imperativo toda vez que permite preservar y custodiar la integridad de uno de los activos más valiosos de la industria: los registros de información sobre sus consumidores financieros, colaboradores, transacciones, oferta de productos, secretos comerciales, propiedad intelectual e investigación, entre otros. Por tal razón, la expedición de la Circular Externa 007 de 2018 representa el principal hito en el fortalecimiento de las prácticas de gestión de ciberseguridad a nivel local y lo que sigue ahora es concentrar los esfuerzos de supervisión en examinar el grado de homogeneidad en su implementación, considerando las particularidades de las diferentes industrias.

Así, y conforme a la perspectiva anual de riesgos emergentes y prioridades de supervisión publicada por la SFC[120] (marzo 2019), la promoción de la gestión de riesgos asociados a la transformación digital y las actividades de supervisión estarán enfocadas en evaluar la robustez de la gestión de riesgos de las entidades que planeen lanzar productos innovadores y lograr que estos nuevos desarrollos estén acompañados de una gestión apropiada de estos. Frente a una eventual exacerbación del riesgo de lavado de activos y financiación del terrorismo (LA/FT) que pueda emerger del uso de las nuevas tecnologías es necesario seguir avanzando en la implementación de mejores prácticas para la prevención de este riesgo, incluida la adaptación de los cinco procesos de debida diligencia y conocimiento del cliente al uso de sistemas de identificación digital. Se busca, además, fortalecer la cooperación internacional mediante la celebración de convenios con organismos nacionales e internacionales para compartir alertas, información y buenas prácticas; así como promover campañas de sensibilización con la industria y el fortalecimiento de las competencias de los supervisores a través de programas de certificación internacional en la materia, entre otros.

Como proceso de seguimiento de la implementación de los lineamientos en materia de gestión del riesgo, se evaluarán las pruebas que realicen las entidades sobre gestión de incidentes y se coordinarán ejercicios sectoriales que fortalezcan los planes de resiliencia del sistema financiero.

Finalmente, la SFC no descarta llevar a cabo inspecciones y pruebas específicas para analizar la situación individualizada, es decir, qué procesos internos se tienen para frenar cualquier ataque y, de producirse, cómo se actúa para solucionar el problema en el menor tiempo y daño posibles; qué controles se realizan sobre los proveedores de tecnología o servicios; en qué se están invirtiendo y con qué objetivo; y cómo se lleva a cabo la integración de todos los sistemas, entre otros aspectos. Gran parte de la discusión se

centra en la importancia del factor humano, es decir, desde la falta de conocimientos y competencias de los consejos de administración y del personal hasta las dificultades para capturar y retener profesionales expertos en el tema, más allá de los aspectos técnicos asociados a los mantenimientos de *software y hardware*.

Perspectivas en materia de ciberseguridad

La convergencia hacia el entorno digital es una realidad imparable que representa una gran oportunidad para el crecimiento económico del país. Debemos seguir avanzando en el reconocimiento especial del riesgo y el establecimiento de procesos generales y específicos de salvaguarda frente a los nuevos riesgos que comporta esta transición.

El desarrollo y fortalecimiento de los mecanismos de protección y defensa contra los riesgos inherentes a estas realidades implica un trabajo mancomunado entre los diferentes actores que se beneficien del entorno digital. Evitar la exposición es una tarea imposible, pero se debe concientizar a los diferentes actores y trabajar de manera conjunta en la creación e implementación de respuestas adecuadas a estos riesgos.

La experiencia ha mostrado que no existe un marco regulatorio ideal o propicio dada la dinámica cambiante del riesgo cibernético. Sin embargo, es necesario revisar y analizar continuamente las estrategias para la gestión de este. Para lograr dicho propósito es fundamental fortalecer y fomentar herramientas de cooperación entre países, instituciones, supervisores y demás actores del entorno digital.

El desafío es permanente en la medida en que la evolución tecnológica margina los desarrollos regulatorios. Es necesario adoptar prácticas de mejora continua entre los actores del entorno digital, desarrollar buenas prácticas para la identificación, prevención y respuesta a los incidentes de seguridad y promover una supervisión dinámica de los diferentes sectores. El riesgo cibernético se adapta a los cambios de la regulación, de ahí la necesidad de enfocar los esfuerzos en desarrollar marcos que permitan gestionarlos bajo principios y lineamientos lo suficientemente flexibles.

La experiencia frente a la ciberseguridad ha demostrado que el crimen cibernético transciende fronteras y jurisdicciones. Cada vez es más habitual que se cometan delitos a través de plataformas o sistemas alojados en diferentes países, por lo que se vuelve imprescindible la cooperación internacional.

En este aspecto adquiere especial relevancia la necesidad de fomentar espacios de cooperación regulatoria (alineación legislativa) y distribución de información —a través de figuras como los Centros de Respuesta a Incidentes de Seguridad (CSIRT)—, que permitan una adecuada gestión de incidentes y una gestión proactiva de este tipo de amenazas.

Los retos que vienen están asociados a consolidar todas las herramientas regulatorias hasta ahora definidas mediante un ejercicio de implementación responsable que implique el desarrollo de competencias para la adecuada gestión del riesgo, la calificación de los actores responsables de estas actividades, la generación de iniciativas de mejora continua y la construcción de estructuras de proyección conjuntas e integradas entre los distintos actores.

Ventajas y retos de las aplicaciones móviles en el sector financiero colombiano

Sandra Rueda, Mario Linares-Vásquez, Camilo Andrés Ortiz-Casas

Introducción

En la actualidad, el uso de dispositivos y aplicaciones móviles ha permeado el vivir diario de las personas. Un reporte reciente de tendencias del Centro de Investigaciones Pew[121] estima que cerca de 2.500 millones de personas a nivel mundial tienen celulares inteligentes, con un porcentaje de penetración que varía entre 76% en países con economías desarrolladas y 45% en países con economías emergentes[1]. Este estudio también señala que, aunque el porcentaje de personas con teléfonos inteligentes ha crecido tanto en países con economías desarrolladas como en países con economías emergentes, la edad es un factor determinante; en particular, las generaciones más jóvenes presentan mayor tendencia a ser consumidores asiduos de apps (aplicaciones móviles) y contenidos digitales.

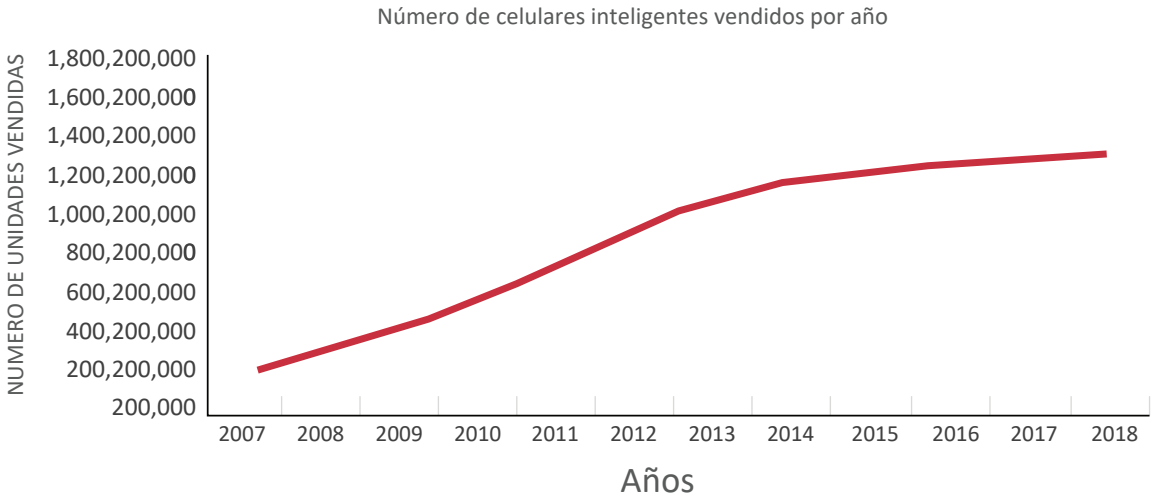
Desde la aparición de las primeras tiendas de apps en 2008, App Store y Android Market (hoy día Google Play), el número de aplicaciones disponibles en las tiendas y el número de descargas ha crecido gradualmente. Mientras el número de aplicaciones disponibles en las dos tiendas en 2008 era 2800, actualmente alcanza 4.900.000 y el número de descargas alcanzó 194.000 millones en 2018[2]. El tipo de aplicaciones disponibles también ha variado, inicialmente había aplicaciones que permitían adicionar funciones sencillas al teléfono, como la calculadora o la libreta de contactos, más tarde aparecieron aplicaciones que permitían manejar mensajería y búsqueda de información en línea, hasta llegar recientemente a aplicaciones especialmente diseñadas para "comprender" al usuario y mejorar su experiencia en campos variados. Uno de los campos que ha generado mayor interés es el financiero; las aplicaciones móviles han sido fundamentales para extender los servicios financieros clásicos permitiendo que los usuarios realicen operaciones, transacciones y solicitudes de servicios y productos en cualquier momento y desde cualquier lugar, reduciendo tiempos de respuestas, eliminando tiempos de espera y facilitando las comunicaciones. Es tal el interés, que el número de descargas de apps financieras a nivel global alcanzó 3.400 millones en 2018[2].

Dado que el crecimiento del mercado de apps está relacionado directamente con el crecimiento del mercado de celulares inteligentes a continuación presentamos un resumen del crecimiento de los dos mercados a lo largo de los últimos años. El número de usuarios en ambos casos ha crecido de forma gradual y las cifras reportadas muestran el alcance actual, así como el potencial, de estas tecnologías.

El mercado de celulares inteligentes

En materia de números y estadísticas, el ecosistema móvil revela gran crecimiento tanto en el caso de dispositivos como en el caso de aplicaciones. La Ilustración 1 muestra esta tendencia en el caso de dispositivos móviles; de acuerdo con Gartner, los fabricantes de celulares inteligentes alcanzaron 1.555 millones de unidades vendidas a nivel mundial en 2018[3]. Desde 2011 la tasa de crecimiento anual siempre ha sido positiva y el número de unidades vendidas en 2018 muestra el gran tamaño del mercado global de celulares inteligentes.

Ilustración 1. Número de celulares inteligentes vendidos a nivel global (cifras de Gartner [4] [3]).

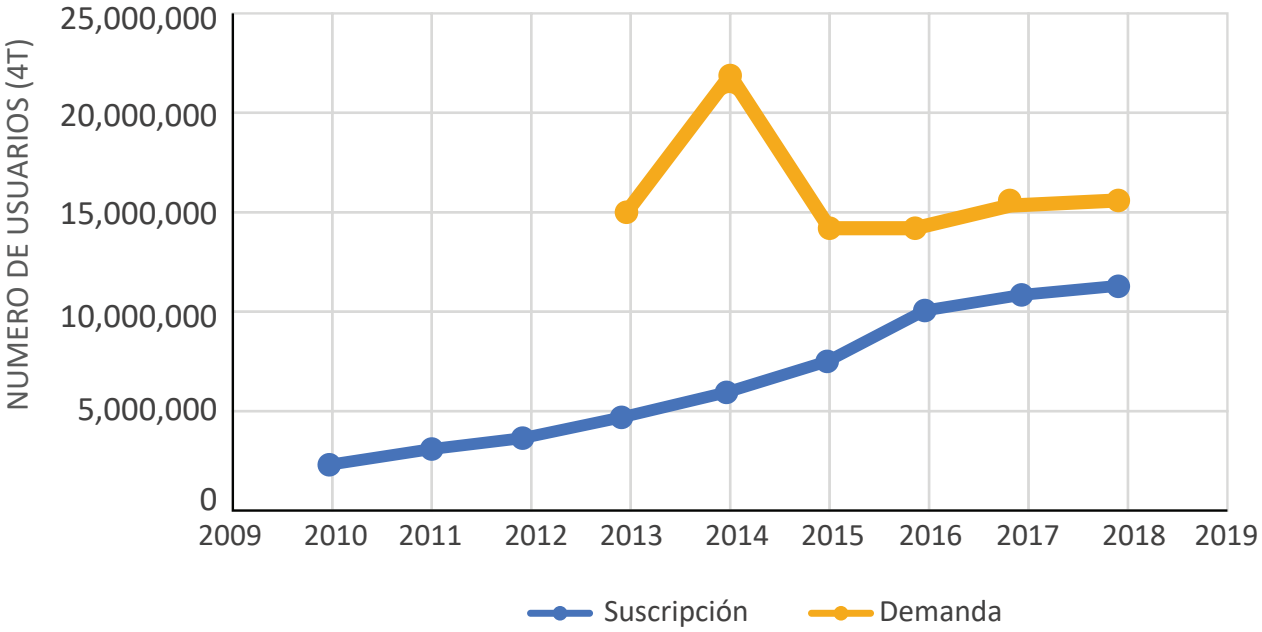


Año	Unidades Vendidas	Tasa Anual de Crecimiento
2010	298.846.600	
2011	471.742.500	57.8%
2012	680.108.200	44.1%
2013	967.775.800	42.2%
2014	1.244.739.800	28.6%
2015	1.423.900.300	14.3%
2016	1.495.959.000	5%
2017	1.536.535.500	2.7%
2018	1.555.267.000	1.2%

Por otro lado, los datos también muestran una disminución en la tasa de crecimiento anual en los últimos años: entre 2011 y 2014 la tasa estuvo por encima de 28%, en 2015 pasó a 14%, en los últimos tres años ha estado por debajo de 10% y ha llegado al mínimo en el último año. Los analistas estiman que el mercado de teléfonos celulares inteligentes y dispositivos tipo ultramobile (dispositivos livianos y de tamaño mediano, entre ellos, tabletas, laptops livianos y convertibles) no crecerá en 2019, pero volverá a crecer en 2020[5]. A pesar de la desaceleración, tanto las cifras de los años anteriores, como la proyección para 2020 muestran la dimensión del mercado de celulares inteligentes y, como consecuencia, la dimensión del mercado de aplicaciones móviles.

La perspectiva de uso masivo de dispositivos móviles es similar en el caso colombiano. El Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) informó que, para 2017, 72% de los hogares colombianos contaban con un teléfono celular inteligente. Estos dispositivos son "los equipos a los que más acceso tienen los hogares" en Colombia[6]. Además, MinTIC, por medio de sus boletines trimestrales, ha reportado un crecimiento gradual del número de suscriptores a internet móvil[122]. Esta cifra en el cuarto trimestre (4T) de 2010 era de 1.708.633 usuarios y ha crecido hasta alcanzar 11.650.489 de usuarios en 2018, es decir, 25,6% de los 45,5 millones de colombianos[7]. La Ilustración 2 resume las cifras reportadas por MinTIC sobre el número de usuarios por suscripción y por demanda en sus boletines del cuarto trimestre (4T) de los años 2010 a 2018.

Ilustración 2. Número de suscriptores a internet móvil en Colombia por año (cifras de MinTIC [8] [9]).

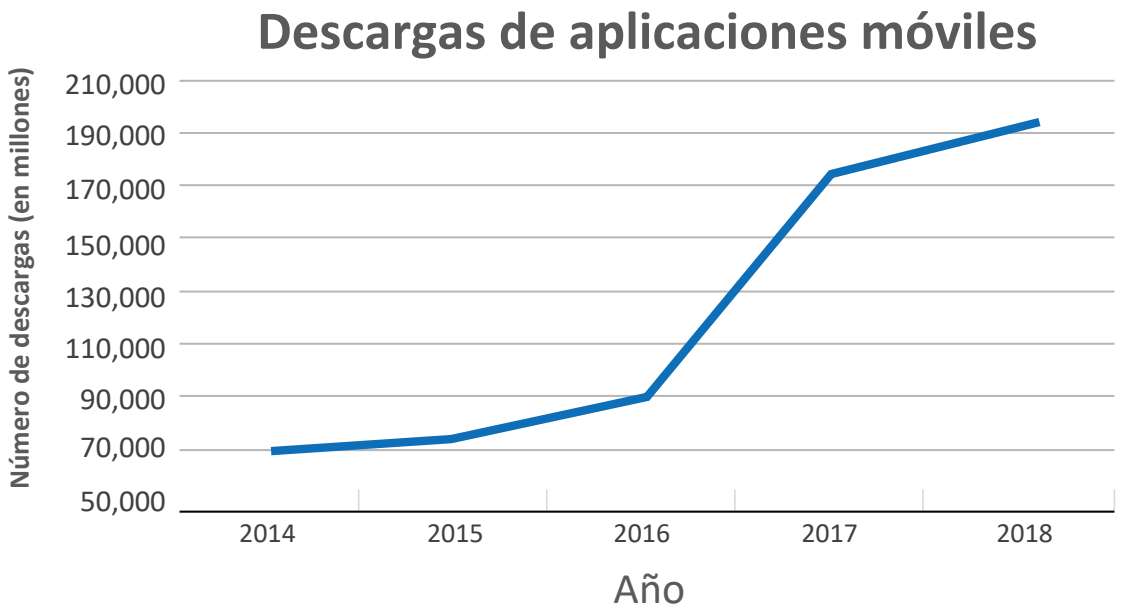


Aunque es más complicado interpretar el significado del número de usuarios por demanda[123], dado que no sigue una tendencia, sabemos que al terminar el cuarto trimestre de 2018 era 14.701.347[8]. Considerando la suma de los usuarios de internet móvil por suscripción y por demanda al final de 2018, 60,5% de la población colombiana podía descargar aplicaciones desde sus dispositivos móviles y ejecutarlas.

El mercado de aplicaciones móviles - apps

De forma similar al mercado de celulares inteligentes, el mercado de las aplicaciones móviles (apps) ha crecido consistentemente. Esto no es extraño, considerando la gran variedad de temas que estas aplicaciones pueden abordar, su facilidad de uso y posibilidad de identificar las preferencias de los usuarios y manejar personalizaciones de acuerdo con dicha información. Las apps también presentan ventajas para los proveedores de servicios dado que permiten alcanzar más personas, mejorar la interacción con el usuario, recibir pedidos y quejas rápidamente y recopilar datos que pueden ser procesados para definir mejores estrategias de negocio. La Ilustración 3 muestra el número de descargas de apps por año, incluyendo iOS App Store y Google Play, a nivel mundial. Aunque no todas las aplicaciones descargadas son realmente usadas por los usuarios, el número de descargas confirma el interés del público global por aplicaciones móviles de diversas categorías.

Ilustración 3. Total global de descargas de apps por año (cifras de AppAnnie [10] [11] [2]).



Incluso diferentes gobiernos han respaldado el desarrollo de aplicaciones que apoyen su gestión en diversas áreas. Los Estados Unidos y la Comunidad Europea cuentan con directorios de aplicaciones móviles para sus ciudadanos, www.usa.gov/mobile-apps y ec.europa.eu/ipg/plan/mobile respectivamente. En el caso colombiano, el gobierno nacional, por medio del Ministerio de Tecnologías de la Información y las Comunicaciones, apoya dos objetivos relacionados con el desarrollo y consumo de aplicaciones móviles: (i) la implementación de estrategias de gobierno en línea y (ii) el apoyo a la comunidad para desarrollar el mercado nacional de aplicaciones móviles. La primera iniciativa apoya la apropiación y el uso adecuado de las tecnologías de la información y las comunicaciones (TIC) para la construcción de un gobierno electrónico. La segunda, denominada Apps.co, apoya las iniciativas de negocio con base en TIC, especialmente aquellas que involucran el desarrollo de aplicaciones móviles, a través de capacitación y apoyo a procesos de innovación como ideación, definición de modelos de negocio y prototipado. De forma similar, la Alcaldía Mayor de Bogotá y su programa Gobierno y Ciudadanía Digital publicaron la guía de sitios Web para las entidades de Bogotá Distrito Capital[12]. Además de definir estándares de diseño y de calidad, la guía considera la funcionalidad que se debe ofrecer para dispositivos móviles.

Los números presentados en los reportes elaborados por organizaciones diversas y las iniciativas que diferentes gobiernos han diseñado son evidencia del interés que generan las aplicaciones móviles, como herramientas para ofrecer servicios públicos y privados, y del alcance potencial de esta tecnología.

Aplicaciones financieras

Del gran universo de aplicaciones móviles existentes, las de interés particular para este trabajo son las de corte financiero, es decir las relacionadas con tecno-finanzas o financial technology (fintech). Aunque no hay una definición universalmente aceptada de fintech, el término hace referencia a sistemas que combinan servicios financieros y monetarios con tecnología. Esta combinación incluye servicios bancarios tradicionales con soporte computacional y servicios más novedosos como micro-mecenazgo (crowdfunding), factorización de crédito, redes sociales para manejo de inversiones, recomendaciones automatizadas para inversión, administración de inversiones, banca móvil, métodos alternativos de pago, criptomonedas, cadena de bloques (blockchain), seguros y otros[13].

Las aplicaciones fintech pueden clasificarse en tres categorías de acuerdo con el usuario objetivo: orientadas a la transformación digital interna, orientadas a la transformación digital para los proveedores y orientadas a la transformación digital para el cliente[14]. Las apps han dado particular impulso a la última categoría, es decir aplicaciones orientadas a transformación digital para el cliente, en particular al desarrollo de banca móvil, branchless banking y consejeros automáticos (robo-advisors).

Contexto mundial

A nivel mundial, los bancos tradicionales ven en las fintechs un mecanismo para ampliar cobertura, mejorar servicios y ser parte del movimiento mundial de transformación digital. Por ejemplo, en Estados Unidos el uso de banca móvil creció consistentemente entre 2011 y 2016 y se estimó que en 2017 cerca del 50% de los adultos en ese país usaron un celular para acceder a su cuenta bancaria[15]. La banca móvil también es ampliamente aceptada en Europa; mientras en 2017, 48% de los entrevistados afirmaron haber usado un celular inteligente para hacer tareas bancarias, en 2018 el número subió a 61%[16]. Por otro lado, las fintechs también son vistas como un mecanismo que puede ayudar a promover la inclusión en el ecosistema financiero en países con economías emergentes; en este contexto las apps hacen posible desarrollar soluciones para clientes con poca cobertura financiera, bajos ingresos y residencia en sitios remotos[17] [18] [19].

Hay diferentes áreas de innovación con gran potencial en el contexto de productos y servicios basados en fintech:

- *Atención interactiva al cliente*. El uso de herramientas de fácil acceso para enviar a y recibir información de clientes (ejemplo SMS) reduce el costo y mejora los tiempos de respuesta en los procesos de manejo de quejas y publicación de información. El resultado es mayor uso, confianza y lealtad[19].

- Pagos con celulares inteligentes. El uso de aplicaciones móviles para pagos con bajo costo en datos y almacenamiento reduce las cuentas inactivas y aumenta los casos de uso para pagos[19].

- Finanzas basadas en conexiones. La construcción de la reputación crediticia de una persona a partir de la información recopilada en las redes sociales permite ofrecer programas de crédito a personas con bajos ingresos y poca probabilidad de acceso a créditos en el sistema tradicional cerrando las brechas en flujo de efectivo[19].

- Finanzas basadas en ubicación. El uso de información de satélite y técnicas de aprendizaje de máquina permite construir opciones financieras, como seguros o créditos, para pequeños clientes en poblaciones que no hacen parte del sistema tradicional[19].

- Reducción del riesgo en finanzas no productivas. Las opciones financieras alternativas ofrecen crédito a personas con bajos ingresos, para pagar gastos programados o inesperados, reduciendo al tiempo el riesgo para el financiador[19].

- Finanzas sin limitación por la ubicación geográfica. La disponibilidad de las apps permite a diversas entidades ofrecer servicios financieros sin importar las fronteras o la ubicación geográfica. Aunque, la empresa desarrolladora debe considerar los aspectos legales pertinentes, el único requerimiento físico para el cliente es contar con un celular inteligente y acceso a internet.

- Educación financiera. El uso de aplicaciones móviles educativas, también conocido como mobile-learning, ofrece a los estudiantes acceso al material de forma independiente de tiempo y espacio, permite combinar material visual, audio y lecturas y hace posible la construcción de actividades interactivas. Estas características pueden ser aplicadas en la construcción de conocimiento financiero tanto para la población con acceso a servicios financieros tradicionales como para la población actualmente fuera de dicho sistema.

- Convergencia de tecnologías. El ambiente digital ha permitido la convergencia de diversas tecnologías: *Cloud*, internet de las cosas (*Internet of Things - IoT*), *Blockchain*, Analítica, Inteligencia Artificial, etc. En este ambiente, el ecosistema móvil habilita además la recolección de datos e interacción en línea con el usuario a partir de mecanismos en el dispositivo, como GPS, cámara y giroscopio, permitiendo así "entender" al usuario y ampliar los servicios disponibles como apps para recomendaciones de inversión, generación de alertas y transferencias de fondos en modo sin contacto (contactless).

- Educación sobre seguridad digital. Las tiendas de apps están diseñadas para facilitar el acceso de los usuarios a diferentes apps, generando también la posibilidad de acceso a apps maliciosas. Aunque las tiendas de apps han implementado iniciativas para evaluar las características de seguridad de las aplicaciones que publican y eliminar las apps maliciosas, aún no se cuenta con la tecnología para que estas iniciativas sean 100% efectivas. Como consecuencia, es importante trabajar en el entrenamiento de los usuarios en conceptos básicos de seguridad digital, en particular cuando las apps usadas involucran movimientos de dinero. Por otro lado, los desarrolladores de apps también deben estudiar y comprender cómo implementar las buenas prácticas para desarrollo de aplicaciones móviles seguras.

A continuación, presentamos tres ejemplos, desarrollados por bancos legalmente establecidos, que ilustran el potencial de aplicaciones fintech que ofrecen productos y servicios en países con economías emergentes:

- El banco Siddhartha Bank, uno de los bancos comerciales en Nepal[124], ofrece *branchless banking* para llevar servicios bancarios a una de las villas, más remotas del país, sin acceso a un sistema bancario formal. Para desplegar el servicio el banco asignó corresponsales/agentes que ejecutan las transacciones en representación del banco por medio de tabletas, máquinas POS (*Point of Sale*) y un mecanismo de autenticación basado en una tarjeta con una franja magnética y huellas digitales[125].

- El banco Union Bank of India[126] también ofrece *branchless banking*. Como en el caso anterior, el banco asignó corresponsales bancarios que le permiten llegar la población de las a las villas más remotas y pobres[127].

- El banco Dubai Islamic Bank[128], con sucursal en Pakistán, ofrece *branchless banking* con el objetivo de ofrecer a sus clientes la posibilidad de realizar transacciones bancarias de una forma cómoda y conveniente por medio de canales alternativos para el servicio[129].

Adicionalmente, cabe resaltar el caso de los bancos totalmente digitales. Aunque algunos bancos han implementado servicios que permiten a sus clientes hacer transacciones por medio de canales remotos vía internet y aplicaciones móviles, los bancos totalmente digitales no cuentan con sucursales, atienden todos los requerimientos y transacciones, incluso la creación de cuentas, por medio de *apps*. Revolut[130] y N26[131] son ejemplos de estos bancos totalmente digitales: cada uno ofrece una aplicación para celulares inteligentes que permite a los clientes abrir y gestionar su cuenta, recibir notificaciones instantáneas de las transacciones que involucran su cuenta, controlar las tarjetas y hacer pagos en diferentes tipos de divisas. Revolut, además, ofrece manejo de criptomonedas.

Por otro lado, entre las aplicaciones fintech desarrolladas por empresas fuera del ecosistema financiero tradicional podemos encontrar productos y servicios para fomentar el compromiso de los clientes por medio de una interacción constante con ellos, habilitar pagos por medio de teléfonos inteligentes y alcanzar poblaciones excluidas del sistema financiero tradicional por su bajo ingreso. Algunos ejemplos son:

- Arifu en Kenia, en alianza con proveedores de servicios financieros (*Financial Service Provider - FSP*), usa mensajería móvil para enseñar a sus clientes de bajos ingresos sobre definición de objetivos financieros y expansión de un negocio, al final de cada módulo de aprendizaje, un cliente puede hacer una evaluación para medir su progreso. Uno de los objetivos de Arifu es mejorar el alcance y compromiso de los clientes con servicios y productos financieros[19].

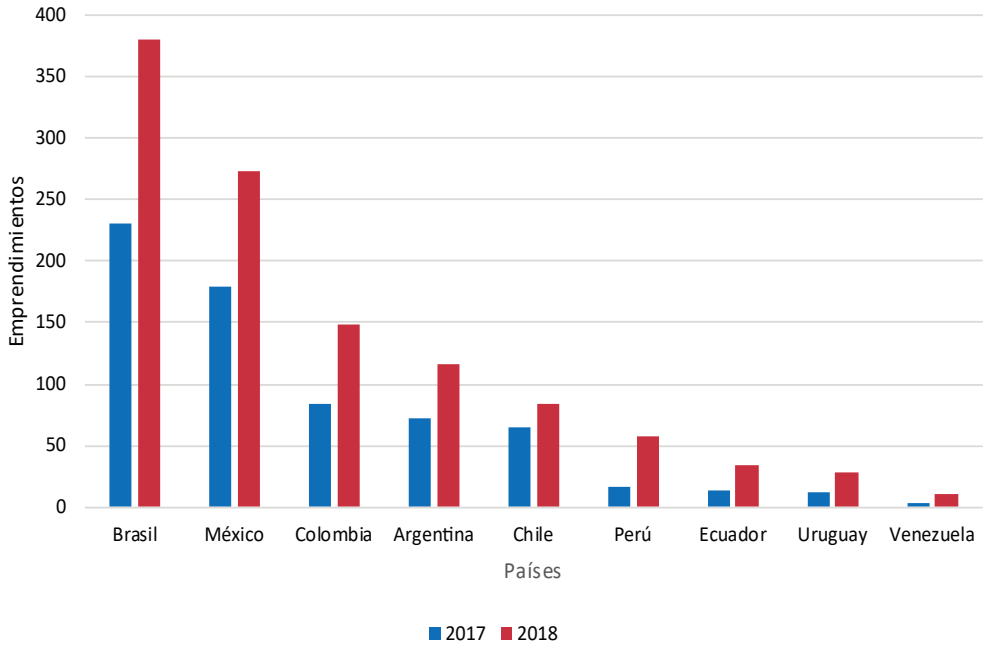
- People's Pension Trust en Ghana es una compañía legalmente autorizada para el manejo de pensiones de trabajadores informales. El éxito de la propuesta depende de la interacción constante con sus clientes para fomentar el ahorro por medio de una aplicación móvil[19].
- Social Lender en Nigeria ofrece crédito a personas con bajo ingreso, que no calificarían para un préstamo bancario. La compañía construye el estudio de crédito de una persona con base en la información de los contactos en redes sociales, incluso en algunos casos dichos contactos aceptan respaldar parte del préstamo (como fiadores)[19].

Los ejemplos presentados ilustran el interés, tanto de las entidades que hacen parte del sistema bancario tradicional como de entidades por fuera de dicho sistema, por desarrollar aplicaciones fintech que permitan ampliar su cobertura, mejorar los servicios y potencialmente crear nuevos modelos de negocio.

América Latina

El Banco Interamericano de Desarrollo (BID), en un estudio de 2018, identificó 1.166 emprendimientos fintech en 18 países de América Latina. La Ilustración 4 presenta los nueve países con el mayor número de emprendimientos en 2017 y 2018. Brasil, México, Colombia, Argentina y Chile agrupan el 86% del total de esos emprendimientos. Los segmentos de pagos y remesas, préstamos y gestión de finanzas empresariales, concentran el mayor número de emprendimientos: 285, 208 y 181 emprendimientos respectivamente (de los 1.166 identificados en 2018) [20].

Ilustración 4. Número de emprendimientos fintech en América Latina (cifras del BID[20]).



En Colombia, el MinTIC ha abordado los temas relacionados con las aplicaciones *fintech* considerando diferentes aspectos, entre los cuales podemos mencionar: (i) digitalización de la banca y regulación de las aplicaciones *fintech*[132], (ii) soporte al desarrollo de las aplicaciones *fintech*, y (iii) perspectivas de las aplicaciones *fintech*[133]. Además, en Colombia existe Colombia *fintech*, una asociación de más de 90 fintechs, que busca el desarrollo de un ecosistema innovador, de la mano del sector financiero y el gobierno colombiano, para ofrecer productos/servicios seguros y con transparencia[134].

Con el fin de mejorar la comprensión que tenemos de la naturaleza del mercado de Apps fintech en Colombia, realizamos un análisis exploratorio con base en la información disponible en el mercado de aplicaciones oficiales Android (Google Play). Para este análisis utilizamos una técnica conocida como *scraping*, que consiste en obtener de forma automática la información disponible en formato HTML en páginas web. El scraping consiste en enviar peticiones HTTP de forma automatizada con el fin de obtener el contenido HTML y luego recorrer dicho contenido para extraer (también de forma automática) las partes de interés. En nuestro caso, extrajimos información disponible en las páginas de producto de producto de las apps Android, publicadas en la categoría "Finanzas" para usuarios en Colombia. La consulta realizada en abril de 2019 mostró que, a ese momento, 210 aplicaciones estaban disponibles en Google Play para Colombia. Es relevante mencionar que una búsqueda hecha desde otro país arrojaría resultados diferentes.

Para este proceso de extracción, creamos un programa en Python, que obtuvo el contenido HTML de las 210 apps en la tienda Play Store, y usamos la librería BeautifulSoup4 para extraer los metadatos principales (nombre, URL de la Play Store, nombre del paquete de instalación, desarrollador, tamaño, número de instalaciones, comentarios, precio y descripción). El texto extraído fue preprocesado, limpiando términos prescindibles (*stop words*) de la cadena de texto obtenida, y luego transformado a caracteres Unicode. Para obtener los archivos APKs de las aplicaciones (es decir el código ejecutable de las apps), usamos la herramienta gplaycli, que descarga los archivos APK emulando un dispositivo. Luego usamos el programa APKTool para recuperar los archivos de la aplicación en una representación intermedia llamada SMALI, que nos permite analizar código de las aplicaciones sin necesidad de recuperar el código fuente original.

Ilustración 5. Aplicaciones agrupadas por propósito

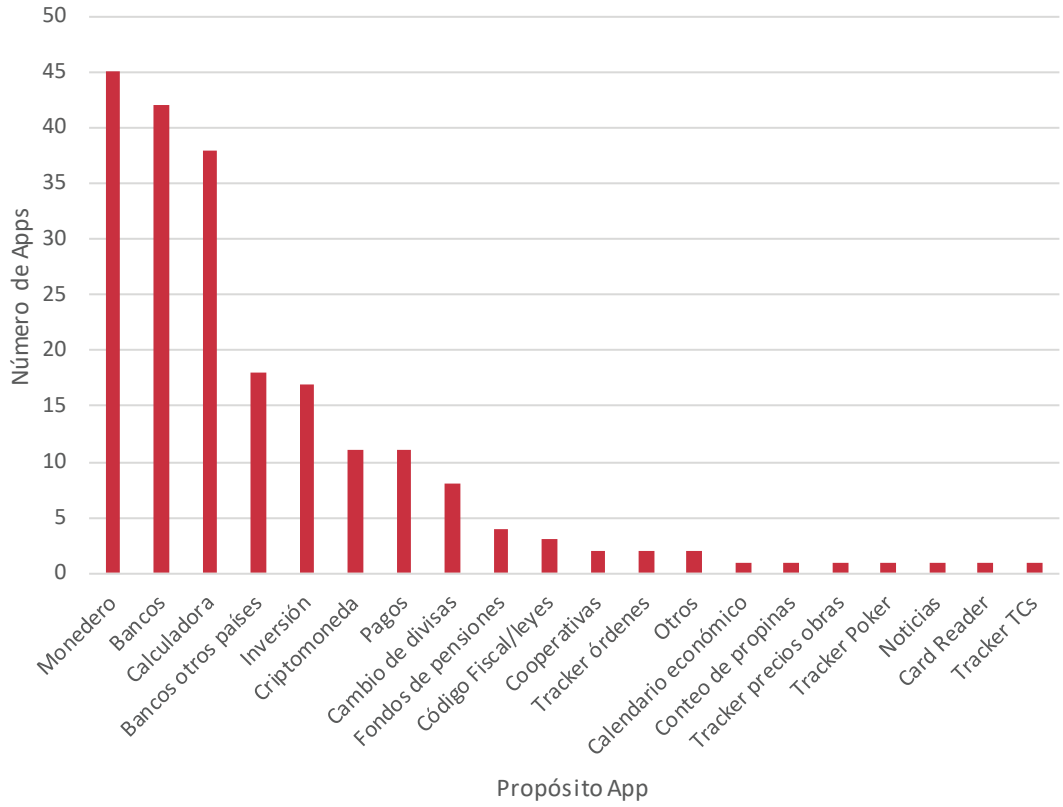


Ilustración 6. Aplicaciones agrupadas por calificación

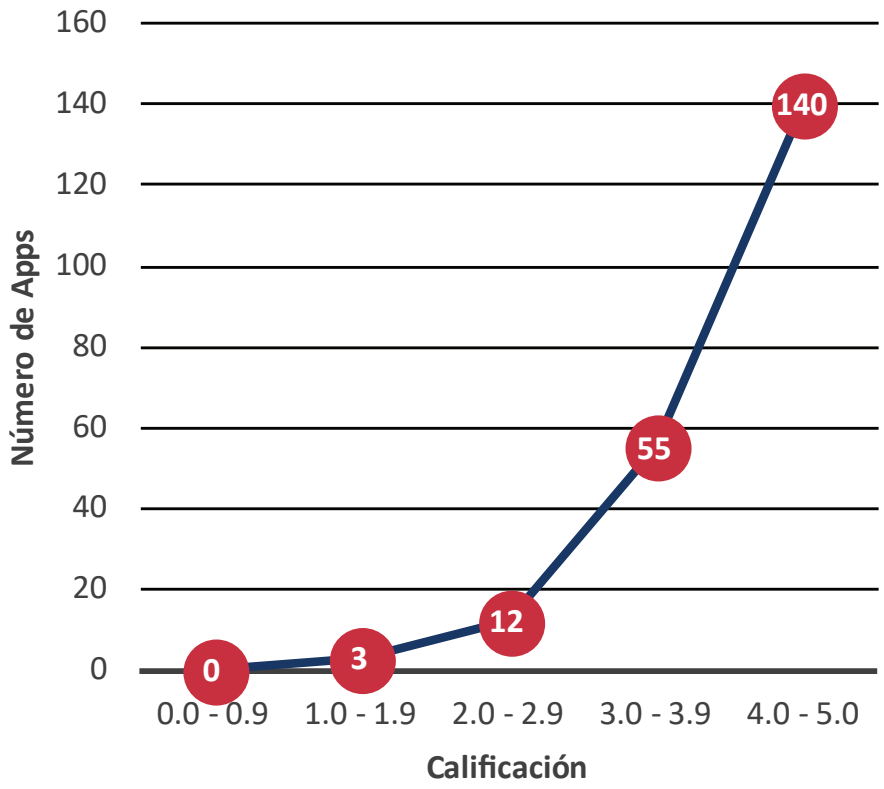


Ilustración 7. Aplicaciones agrupadas por tamaño

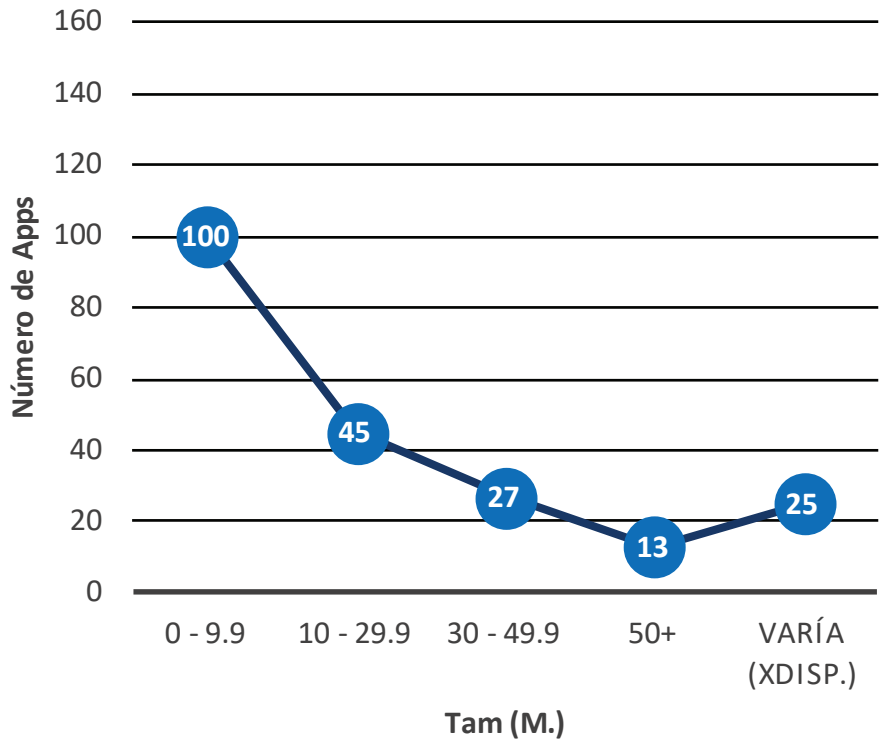
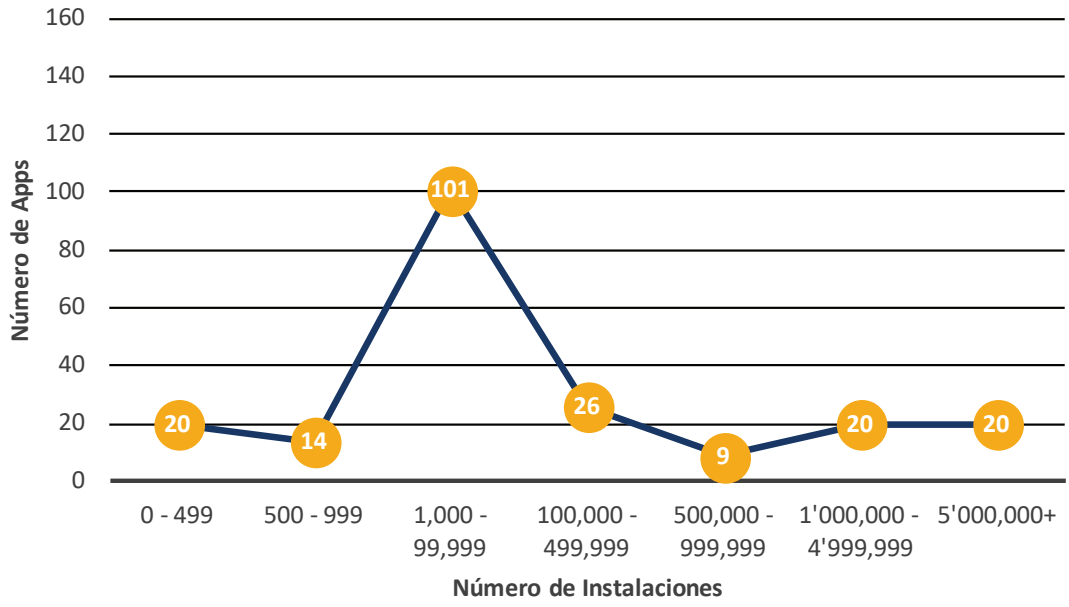


Ilustración 8. Aplicaciones agrupadas por número de instalaciones



La Ilustración 5 muestra la distribución de las 210 apps de acuerdo con su propósito. Para identificar el propósito, analizamos manualmente el contenido textual de la descripción y en algunos casos instalamos las apps en dispositivos virtuales para ser exploradas manualmente. Las apps financieras más comunes en el caso colombiano son monederos, aplicaciones de bancos, calculadoras, bancos de otros países, apps para inversión, criptomonedas y manejo de pagos. Estas aplicaciones agrupan el 86% de las 210 aplicaciones identificadas. Cabe aclarar que estas 210 apps no incluyen el conjunto de apps desarrolladas por empresas colombianas pero publicadas para otros países, es decir, este análisis es solo para las apps distribuidas en Colombia vía Google Play, hayan sido desarrolladas o no en Colombia.

Un caso particular para discutir, es que en las 210 apps analizadas, hay aplicaciones de "bancos de otros países" disponibles para usuarios colombianos. Los mercados de distribución de apps, permiten a los desarrolladores de apps seleccionar los países o regiones de distribución al momento de publicar su aplicación; es posible que en el caso de estas aplicaciones de "bancos de otros países", los desarrolladores hayan escogido una estrategia de distribución más global a pesar de no prestar servicios en Colombia, o pudo ser simplemente un error en la selección. Como no hay control directo en los mercados con respecto a la región asociada con una aplicación, es decir dónde se puede publicar y dónde no, es posible que un usuario pueda acceder a aplicaciones de otros lugares (benignas y malignas) creyendo que están habilitadas para Colombia.

Adicionalmente al propósito de las apps, extrajimos el número de instalaciones (Ilustración 8), tamaño de la aplicación en Mega bytes (Ilustración 7) y calificación promedio de cada app (Ilustración 6). Aunque los datos de instalación, sin tener la tasa de desinstalación, no revelan el uso real de las apps, los números muestran que los usuarios en el mercado colombiano están interesados en el uso de apps relacionadas con la categoría "Finanzas". Algunos de los hallazgos son los siguientes:

- Con respecto a la calificación promedio dada por los usuarios a las 210 aplicaciones. El 92% de las aplicaciones (195) han recibido calificaciones iguales o mayores a 3/5 indicando una aceptación positiva por parte de los usuarios; 140 se encuentran en el rango de 4 a 5 estrellas, 50 en el rango de 3 a 3.9 estrellas y 15 apps se encuentran por debajo de las 3 estrellas.

- 69% de las aplicaciones (145) tiene un tamaño menor o igual a 30M. En general, se espera que las aplicaciones móviles no tengan tamaños grandes para contribuir a conservar el espacio de almacenamiento de los usuarios en los dispositivos. El espacio ocupado por aplicaciones móviles puede ser atribuido en su gran mayoría a recursos como imágenes o videos incluidos en los archivos APK. Las librerías externas también contribuyen al tamaño de una app; durante el proceso de compilación de una aplicación Android, el código de las librerías (compilado o no) se incluye en el mismo archivo APK[21].

- Solo 19% de las aplicaciones (40) han sido instaladas más de 1.000.000 veces, 35 se encuentran en el rango de 100.000 a 999.999 instalaciones, 101 apps han sido instaladas entre 1.000 y 99.999 veces y tan solo 34 han sido instaladas menos de 1.000 veces. Como era de esperar, las 40 apps más instaladas han sido bien calificadas por los usuarios; solo una tiene una calificación inferior a 3.5. Por otro lado, de las 40 aplicaciones hay nueve de bancos extranjeros y 31 están asociadas con negocios en Colombia o son globales, pero pueden ser usadas por colombianos. De estas últimas 31 hay nueve desarrolladas para bancos, todas bien calificadas (con una calificación igual o superior a 3.5); entre las 22 restantes hay cuatro apps para pagos en línea, siete asociadas con banca de inversión, tres para manejo de criptomonedas, siete son monederos y una presenta información para cambio de divisas.

- De las 210 aplicaciones, 162 aplicaciones no están relacionadas con en el sistema financiero (es decir, no son aplicaciones de entidades financieras). En nuestro análisis encontramos que las 162 apps se distribuyen por categorías así: aplicaciones para llevar registro de gastos diarios/mensuales (45), calculadoras para diferentes propósitos tales como créditos, mesadas, fondos de retiro y cálculos convencionales (38), apps de bancos de otros países (18), simuladores financieros (17), y criptomonedas (11). El 14% restante se distribuye en calendarios fiscales, contadores de propinas, códigos fiscales/leyes, conversores de monedas, entre otros.

Retos

El uso de las fintech es un ejemplo de innovación que puede convertirse en un arma de doble filo; para los usuarios, para los creadores de estas y para las entidades interesadas en ofrecer sus servicios financieros/bancarios a través de canales digitales y no "tradicionales". Sin lugar a duda hay ventajas para todos los actores (usuarios, creadores y desarrolladores) y para el sector en general, incluyendo a los gobiernos que regulan los sistemas financieros. Sin embargo, el uso y la implementación de fintechs presenta ciertos retos (internos, externos y técnicos) para la sociedad.

En un estudio reciente del Grupo Consultor para Asistir a los Pobres (*The Consultative Group to Assist the Poor*), se evaluaron 18 proyectos piloto basados en aplicaciones fintech, para determinar los retos (internos y externos) que contribuyen o afectan el éxito de una idea basada en tecnología fintech. A continuación describimos esos retos.

Los retos internos agrupan aspectos relacionados con el desarrollo y funcionamiento de la aplicación, tales como[19]:

- Desarrollar una propuesta de valor apropiada para el mercado. Esto requiere un análisis cuidadoso para comprender al cliente objetivo y responder a sus necesidades, y la ejecución de pruebas para evaluar el valor real de la propuesta antes de su lanzamiento.

- Ensamblar los recursos humanos y tecnológicos apropiados. Aunque no es una recomendación nueva, el estudio encontró que algunas empresas desarrolladoras de fintechs no consideran este aspecto desde una etapa temprana en la construcción de su empresa.

- Encontrar el balance entre interacción digital y personal. Los clientes objetivo de muchas fintechs no están familiarizados con los servicios bancarios y menos con la tecnología que puede soportar estos servicios. Como consecuencia, el primer paso es ayudarles a sentirse cómodos usando dichos servicios.

- Formar alianzas estratégicas. Si no se cuenta con el capital necesario para comenzar, puede ser conveniente crear una alianza con proveedores de servicios bancarios, organizaciones no gubernamentales (ONG) o instituciones de micro-finanzas.

Los retos externos agrupan aspectos relacionados con el ecosistema, incluidas fuentes de financiación y regulación[19]:

- Apoyo financiero. Puede ser difícil encontrar empresas dispuestas a financiar ideas y modelos de negocio nuevos por la incertidumbre y el riesgo asociados.

- Despliegue. No es suficiente tener una idea novedosa, es necesario construir el soporte logístico adecuado para poder construir y mantener una empresa con base en dicha idea.

- Regulación. Dado que muchas fintechs presentan modelos nuevos de negocio, la regulación usualmente no los considera. Esto puede llevar a poner a los usuarios de las aplicaciones en riesgo por la falta de regulación, o puede ser una barrera para la innovación porque la regulación es muy estricta para los productores de apps. La regulación también aplica en lo concerniente al manejo de la privacidad, integridad y confidencialidad de los datos, tanto personales como de las transacciones.

Adicionalmente a los retos internos y externos, un estudio de la Universidad de Florida identificó cuatro retos técnicos[22]:

- Algoritmos débiles de cifrado a nivel de red. Las redes celulares de segunda generación 2G GSM pueden ser ideales si se considera el despliegue, dado que tienen amplio cubrimiento a nivel mundial, pero son problemáticas si se considera la seguridad de la información porque ofrecen algoritmos de cifrado débiles.

- Autenticación de los elementos de red. Las redes GSM manejan autenticación del dispositivo a la red, pero no de la red al dispositivo. Esto significa que una estación maliciosa podría recibir toda la información en una zona.

- Algoritmos de cifrado a nivel de aplicación. Las redes 3G, 4G y los celulares inteligentes pueden soportar seguridad de extremo a extremo (*end-to-end*) reduciendo los problemas identificados en las redes 2G. Sin embargo, en las aplicaciones que corren con base en las plataformas más nuevas, los problemas de cifrado se presentan a nivel de aplicación; en el uso de protocolos o configuraciones inseguras.

- Privacidad. Mientras un banco tradicional tiene la información de sus usuarios, en los contextos nuevos, que incluyen redes de pares (peer-to-peer), múltiples usuarios pueden ver las interacciones de otros usuarios y las empresas que desarrollan las fintechs pueden recopilar los datos de los usuarios, en muchos casos sin presentar una política de manejo de datos privados.

El análisis exploratorio de las aplicaciones disponibles en Google Play para Colombia muestra cómo la disponibilidad de aplicaciones fintech vía mercados de alto acceso, sin costo en algunos casos, puede ser un riesgo para los usuarios, dado que la falta de educación y conocimiento puede llevarlos a instalar aplicaciones que no tienen nada que ver con el ecosistema fintech del país y que incluso pueden ser aplicaciones maliciosas que buscan atentar contra la privacidad y confidencialidad de la información de los usuarios. Es necesario entonces, construir y promover una cultura colombiana y latino americana de investigación y análisis más profunda con respecto a los retos, vulnerabilidades y riesgos asociados con el uso de esta tecnología.

Aspectos técnicos de las apps financieras

Múltiples guías de referencia, listados de buenas prácticas y patrones y gran cantidad de documentos orientados a la concepción, diseño, implementación y pruebas de aplicaciones móviles están disponibles de forma pública. Todas las recomendaciones aplican de forma general para cualquier tipo de aplicación móvil, sin embargo, las apps móviles para fintech presentan condiciones de uso específicas y tienen retos particulares, como lo describimos en la sección anterior. En esta sección describimos aspectos internos y externos que deben ser tenidos en cuenta por compañías interesadas en crear y mantener aplicaciones móviles fintech y en particular por sus equipos de desarrollo.

Aspectos internos

Los aspectos internos son elementos que impactan directamente la calidad de la aplicación desde la parte técnica y del equipo involucrado en el desarrollo de la aplicación. Estos aspectos incluyen decisiones de diseño e implementación de la aplicación y prácticas de proceso tales como ingeniería de usuarios y verificación/validación. Una aplicación móvil exitosa requiere tres elementos: una buena idea, un buen código y un buen diseño[23]. Por otro lado, diferentes aspectos técnicos influyen en la calidad de las aplicaciones móviles y, por ende, en los ratings dados por los usuarios[24] [25]; algunos de estos aspectos son el tamaño de la aplicación, soporte a diferentes versiones de la plataforma de desarrollo, e inestabilidad de las API.

Sin lugar a duda la calidad técnica de una implementación es un factor importante; esto se refleja directamente en la capacidad de la aplicación para proporcionar sus servicios con calidad, es decir, sin fallas percibidas por el usuario. Hablando en términos de ingeniería de software, los usuarios perciben la calidad en (i) la implementación de los requerimientos funcionales (es decir los servicios y funcionalidades proporcionadas) y (ii) en los atributos de calidad proporcionados por el sistema (por ejemplo, usabilidad, disponibilidad, seguridad, tolerancia a fallas). En el caso de aplicaciones fintech es de vital importancia poner atención al cubrimiento de atributos de calidad como seguridad, uso, accesibilidad y disponibilidad, que podrían no ser tan importantes para otros tipos de apps. A continuación, describimos algunos de esos atributos y sus implicaciones en el caso de aplicaciones fintech.[26]

Accesibilidad

Este atributo de calidad implica que cualquier persona, independientemente de su edad, género, discapacidades, conocimientos, etc., debe poder usar una app sin ser objeto de exclusión. Una aplicación fintech debe asegurar que su segmento de usuarios objetivo puede usar la app, en particular aquellos usuarios que por algún tipo de discapacidad (visual, auditiva, motora, cognitiva) puedan encontrar inconvenientes a la hora de usar aplicaciones. De acuerdo con el *World Report on Disability* de la Organización Mundial de la Salud[27], en el 2011 cerca del 15% de la población mundial vivía con algún tipo de discapacidad. Adicionalmente, el portal de estadísticas de discapacidades de la Universidad de Cornell reporta que 12.9% de mujeres y 12.7% de hombres de todas las edades en Estados Unidos tienen una discapacidad [28]. Esto sugiere que los desarrolladores de aplicaciones, en general, deberían preguntarse si sus aplicaciones son accesibles y preocuparse por (i) seguir las guías de accesibilidad disponibles, (ii) hacer uso de los servicios y funcionalidades de accesibilidad (por ejemplo, TalkBack en Android y VoiceOver en iOS) proporcionados por las plataformas existentes y, finalmente, (iii) incluir usuarios con discapacidades en los procesos de diseño y pruebas.

Compatibilidad

Este atributo involucra dos características: (i) fragmentación y (ii) desarrollo multiplataforma. La fragmentación hace referencia a las diferentes versiones de pantallas, hardware, sistema operativo y API que se pueden encontrar en la misma plataforma[29]. Por ejemplo, en el caso de Android, en la actualidad hay 29 versiones diferentes de la API de Android y del Sistema Operativo y 96,2% de los dispositivos en el mundo (a mayo 7 de 2019) se distribuyen en nueve versiones diferentes del Sistema Operativo[30]; esto quiere decir, que una app Android debería ser compatible con esas nueve versiones (desde *Kitkat* hasta *Pie*) y funcionar sin errores. La segunda característica, la compatibilidad, considera que los usuarios de aplicaciones móviles están distribuidos en dos plataformas dominantes: Android y iOS; por eso las aplicaciones deberían estar disponibles en ambas plataformas, asegurando la misma calidad en términos de errores y asegurando consistencia de comportamiento, es decir, se ofrecen las mismas

funcionalidades tanto para Android como para iOS. En resumen, los desarrolladores de apps deben tener en cuenta la fragmentación y verificar que las apps son compatibles con diferentes dispositivos, tamaños de pantalla, versiones de API y las dos plataformas existentes. Al diseñar y construir una aplicación, los desarrolladores deberían considerar las características de las diferentes plataformas móviles donde dicha aplicación puede ser ejecutada; una aplicación debe conservar una interfaz gráfica consistente sin importar el tamaño de las pantallas del dispositivo en el que está corriendo, ni la API o sistema operativo que tiene el dispositivo.

Tolerancia a fallas

Este atributo de calidad significa que las aplicaciones deben ser capaces de seguir funcionando a pesar de la existencia de una falla en algunos de sus componentes. La tolerancia a fallas requiere diseños e infraestructura que proporcionen alta disponibilidad del lado de los servicios de *backend*[135] y manejo de errores de la aplicación móvil del lado del cliente. En el caso de aplicaciones móviles, cobra vital importancia el manejo de excepciones al comportamiento esperado y el uso de estrategias para mantener la integridad de datos ante cualquier eventualidad. Por ejemplo, los escenarios de conectividad eventual (es decir pérdida temporal o total de conexión a internet) son comunes, por mala señal en lugares específicos o por la falta de acceso a planes de datos. Si estos escenarios no son bien manejados en el lado de la aplicación móvil, pueden afectar negativamente:

- La usabilidad de la aplicación. Si no se manejan mensajes expresivos informando un comportamiento limitado o el bloqueo temporal de la funcionalidad por la falta de conexión. La usabilidad también se ve afectada cuando la aplicación no tiene mecanismos de almacenamiento local (tipo caché) y sincronización automática cuando se recupera la conectividad.

- La integridad de los datos. Si no se implementan transacciones de tipo ACID (Atomicidad, Consistencia, Aislamiento, Durabilidad) es posible terminar generando datos inconsistentes del lado del backend o del lado de la aplicación móvil. Por otro lado, las malas implementaciones de los mecanismos de sincronización pueden llevar a comportamientos inesperados de la aplicación.

Seguridad

Este aspecto es tal vez el más importante, dado que las apps financieras, tienen que asegurar integridad y privacidad de los datos de los usuarios a nivel de datos personales y de sus transacciones. La seguridad de una aplicación móvil no solo depende de la app como tal, sino del manejo de seguridad en todo el ambiente que la rodea, es decir, el usuario, el dispositivo, los canales de comunicación de la app con los servicios de *backend*, y el *backend*. En lo relacionado con usuarios, la falta de educación en medidas de seguridad puede llevar a que el usuario tenga un mal manejo de sus contraseñas, instale aplicaciones maliciosas en su dispositivo o no instale actualizaciones de seguridad vitales para el sistema operativo; es obligación de las compañías que ofrecen las apps ayudar a mejorar la educación de los usuarios. Del lado de la aplicación, los desarrolladores deben asegurar que la app maneja los datos privados del usuario de forma apropiada; cifrando la información cuando se requiera, ya sea para almacenarla o para transmitirla. Esta información (datos personales y transacciones) solo se debe enviar a servidores externos cuando es necesario para ejecutar su función principal, de forma cifrada y solo con consentimiento del usuario. Respecto a los algoritmos usados para cifrado de datos, estos deben ser conocidos y cambiados inmediatamente si alguno de los equipos de investigadores dedicados a la evaluación de algoritmos de cifrado reporta problemas en estos.

Aspectos externos: regulación y estándares

Muchos gobiernos están enfrentando hoy día los retos políticos que aparecen con el desarrollo de las aplicaciones fintech, y las cajas de arena regulatorias (*regulatory sandboxes*) son herramientas que permiten a quienes trabajan en el desarrollo de las políticas observar los comportamientos que emergen, tomar decisiones al respecto y construir política con base en información real. En seguridad, una caja de arena es un ambiente especialmente configurado para ejecutar aplicaciones de forma controlada. La caja da acceso a un conjunto limitado de recursos y controla de forma estricta el tipo de operaciones que es posible ejecutar sobre dichos recursos. En el contexto de aplicaciones fintech, una caja de arena regulatoria es un ambiente creado por un ente regulador para permitir pruebas reales a pequeña escala de conceptos innovadores, promoviendo así el desarrollo de nuevas ideas, permitiendo al ente regulador observar el comportamiento real de la industria y reaccionar con agilidad y garantizando al tiempo la protección del consumidor[31].

La primera implementación de caja de arena regulatoria se dio en 2015 en el Reino Unido[31] y desde entonces un buen número de países en el mundo han usado el mismo concepto. En algunos casos, el ecosistema es más amplio, incluyendo incubadoras y centros de desarrollo, lo cual permite a gobiernos y entes reguladores entender mejor el comportamiento e interacción con otros participantes en el ecosistema de desarrollo. En el contexto de la Unión Europea, además del Reino Unido, otras cuatro autoridades competentes contaban con cajas de arena regulatorias en 2018: Dinamarca, Lituania, Polonia y Países Bajos. Noruega ya había anunciado su implementación, mientras España y Hungría la están considerando[32].

En Asia, Oceanía y África, autoridades regulatorias en India, Malasia, Singapur, Arabia Saudita, Australia, Brunéi, Baréin, China, Hong Kong, Indonesia, Japón, Jordania, Mauricio, Corea del Sur, Rusia, Taiwán, Tailandia y Turquía han anunciado la intención de crear –o ya cuentan con ellas– cajas de arena regulatorias[31].

En Latinoamérica, el BID ha apoyado el desarrollo de marcos normativos que consideren el desarrollo tecnológico y ha sugerido a los gobiernos la creación de bancos de pruebas (cajas de arena regulatorias) con las mismas finalidades ya mencionadas: permitir la interacción entre la industria y los entes reguladores y facilitar la transición para las aplicaciones y los entes de control hacia una supervisión "basada en las verdaderas actividades de la industria"[33]. El Centro de Estudios Monetarios Latinoamericanos (CEMLA), conformado por los bancos centrales de América Latina y el Caribe, menciona que las regulaciones financieras tradicionales pueden ser muy rígidas, limitan la adopción de nuevas tecnologías y demoran mucho para adaptarse, además, son ambiguas o carecen de elementos que regulen las actividades basadas en tecnologías nuevas. Adicionalmente, los marcos regulatorios deben incluir los aspectos importantes en cada contexto, es decir, no es posible construir una regulación que pueda aplicarse a todos los países y a todas las tecnologías. "Dependiendo del nivel de impacto de una innovación fintech en los objetivos de una política pública, el nivel de control y supervisión debe variar".[34]

México ya desarrolló una ley para regular la industria emergente (abril 2018)[136] y Chile anunció que cuenta con un borrador de ley (mayo 2018)[137]. La autoridad competente en Brasil anunció recientemente (junio 2019) su intención de implementar un modelo de caja de arena para responder a la transformación tecnológica en el campo financiero, incluyendo aplicaciones fintech, *Distributed Ledger Technology, Blockchain* e Inteligencia Artificial[138 - 139].

Colombia no es ajena a la necesidad de estudiar y regular las actividades de transformación digital en el campo financiero. La Superintendencia de Industria y Comercio (SIC) ofrece La Arenera, una caja de arena regulatoria que brinda un marco de trabajo para realizar experimentos y pruebas de innovaciones tecnológicas. Además, ofrece elHub y regTech. La primera apoya a entidades interesadas en temas relacionados con la innovación financiera y tecnológica, mientras la segunda aprovecha desarrollos tecnológicos para mejorar sus procesos internos[35] [36].

Recomendaciones para el desarrollo de apps estables y seguras

A la hora de construir aplicaciones para fintech es importante tener en cuenta los aspectos que mencionamos en las secciones anteriores y seguir las guías de diseño e implementación propuestas para cada plataforma de desarrollo. Adicionalmente, los equipos de desarrollo pueden utilizar los recursos que las plataformas de desarrollo y los mercados en línea ofrecen. Por ejemplo, en el caso de Google Play (el mercado oficial para aplicaciones móviles), los desarrolladores pueden hacer uso de Android Vitals[140], un tablero (dashboard) para recolección de información en tiempo de ejecución relacionada con estabilidad y desempeño de la aplicación; otra herramienta disponible para ejecutar pruebas de exploración automática es el *Firebase Test Lab*[141] que adicionalmente ofrece la posibilidad de pruebas en diferentes dispositivos.

Las tiendas en línea también proporcionan mecanismos de ayuda para asegurar la calidad de las aplicaciones móviles. Por ejemplo la App Store de Apple cuenta con un comité de revisión de aplicaciones encargado de validar que una app se ejecute de acuerdo con la guía establecida[142], no tenga problemas de seguridad y no contenga material ofensivo. Este mecanismo permite a la tienda garantizar un estándar mínimo de características de diseño y calidad de la aplicación. En cuanto a seguridad, validan que la aplicación informe y solicite consentimiento si la aplicación requiere acceso a datos del usuario y que no contenga programas que puedan perturbar el funcionamiento normal del sistema operativo o de otras aplicaciones. Por otro lado, Google Play requiere que los desarrolladores firmen su aplicación, para esto el desarrollador debe contar con un par de llaves pública y privada y el correspondiente certificado digital. Este mecanismo permite a la tienda verificar que una actualización futura es auténtica, es decir, proviene del autor original[143]. Google Play no cuenta con un comité de revisión, pero por su política de acceso abierto, decenas de laboratorios de investigación en seguridad de la información pueden evaluar el comportamiento de las aplicaciones y reportar problemas.

A pesar de los mecanismos de control de las tiendas, diferentes adversarios han explotado vulnerabilidades presentes en las apps para obtener información de los usuarios o ganar acceso no autorizado a los dispositivos. En 2015, Apple eliminó aplicaciones legítimas de tiendas oficiales porque contenían *malware*, aunque las aplicaciones no habían sido diseñadas o desarrolladas para ello. Los problemas incluían, por un lado, desarrolladores que habían descargado y usado un IDE de una tienda no oficial que insertaba automáticamente *malware* en las aplicaciones y, por otro lado, desarrolladores que usaron una librería de un tercero que comprometía la privacidad del usuario; esta misma librería era usada por algunas aplicaciones Android con consecuencias similares[37]. En esa medida, los desarrolladores de apps deberían usar herramientas de programación y librerías que provengan de fuentes oficiales y confiables.

Entre las técnicas que los programas de *malware* usan para confundir a los usuarios y lograr ser instaladas encontramos reempaquetamiento (repackaging), actualización y aplicaciones falsas [38]. En el primer caso –reempaquetamiento–, los desarrolladores maliciosos descargan una aplicación real, la decompilan, adicionan nuevas instrucciones o clases maliciosas, generan un nuevo APK y la publican en el mercado oficial o en mercados no-oficiales que no tienen certificación de autenticidad. En el segundo caso –actualización–, los desarrolladores maliciosos siguen el mismo procedimiento, pero las instrucciones se encargan de descargar componentes maliciosos tiempo después de ser instaladas y estar en funcionamiento. En el último caso –aplicaciones falsas–, los desarrolladores maliciosos crean aplicaciones que lucen como legítimas, en particular, pueden obtener los recursos de la aplicación original para usarlos en la aplicación falsa. Para evitar este tipo de ataques, los desarrolladores deben aplicar técnicas para proteger sus aplicaciones, en lo posible, de estas técnicas de ingeniería reversa y preferir la publicación de aplicaciones en tiendas oficiales. Un ejemplo representativo de estás técnicas es la ofuscación (obfuscation) de código, que modifica los nombres de variables y la organización original del código, para que sea difícil para un atacante entender el código original luego de ser decompilado.

Por otro lado, muchas amenazas en el contexto móvil emergen de la interacción entre aplicaciones instaladas en un mismo dispositivo móvil. Esta interacción es deseable porque facilita muchas actividades al usuario; piense, por ejemplo, en una aplicación que registra cuánto ejercicio ha hecho usted en una semana y quiere pasar ese dato a una aplicación que comparte la información con sus amigos[39]. Si un desarrollador no configura los permisos sobre este tipo de servicios de forma apropiada, otras aplicaciones pueden obtener acceso indeseado a la información. Para evitar estos escenarios, los desarrolladores deberían estudiar y comprender cómo controlar los mecanismos que permiten compartir información y usarlos al construir una aplicación. Además, deberían estudiar y conocer los sistemas en los que corren estas aplicaciones, incluso las vulnerabilidades que los afectan; este conocimiento los podría guiar en el momento de desarrollar sus actividades de validación y verificación para identificar los tipos de vulnerabilidades más comunes a nivel de apps y del sistema operativo[26].

OWASP, una organización mundial interesada en mejorar las prácticas para desarrollo de software seguro, está trabajando en el desarrollo del estándar MASVS (*Mobile Application Security Verification Standard*), un marco (framework) que define la línea base de prácticas que deberían ser tenidas en cuenta, tanto por arquitectos como por desarrolladores, al construir una aplicación móvil[40] [41]. El estándar define tres niveles de seguridad: L1 para incorporar en una app protección contra las vulnerabilidades más comunes, L2 para apps que manejan datos sensibles y por tanto requieren prácticas de seguridad más sofisticadas y R para control de ingeniería reversa. Las aplicaciones fintech que manejan datos sensibles de los usuarios, como datos personales y números de tarjetas de crédito, deberían implementar L2+R. Este nivel incluye recomendaciones en las siguientes categorías:

1. Arquitectura, diseño y modelo de amenazas. Identificar explícitamente todos los componentes de la aplicación (incluso lado servidor, lado cliente y comunicaciones), su organización como una unidad y su modelo de seguridad (que incluye clasificación de los datos por su nivel de sensibilidad y modelo de amenazas).

2. Manejo de datos. Entender las restricciones sobre el manejo de datos sensibles, como credenciales y datos privados, durante todo el ciclo de vida de una app, incluyendo comunicaciones entre procesos, almacenamiento en memoria y consideraciones de copias de respaldo (*backups)*.

3. Criptografía. Atender las recomendaciones sobre selección de algoritmos de cifrado y administración apropiada de las llaves de cifrado en la app.

4. Autenticación y manejo de sesiones. Seleccionar cuidadosamente las técnicas de autenticación, considerando diferentes formas de autenticación y autenticación de doble factor. Además, manejar las sesiones de forma apropiada, incluyendo manejo de estado cuando sea necesario, protección de tokens de identificación de sesión, validación de información de sesión en el lado servidor, expiración y cierre.

5. Comunicaciones. Implementación de técnicas de protección de comunicaciones, en particular manejo de cifrado e integridad por medio de TLS y uso y validación de certificados.

6. Interacción con plataformas. Solicitar el conjunto mínimo de permisos necesarios para cumplir con la funcionalidad de la aplicación, utilizar filtros para los datos de entrada generados por fuentes no confiables y restringir el acceso a funciones sensibles de la aplicación y al uso de WebViews.

7. Calidad. La app ha sido construida en modo release, eliminando todas las características usadas en modo depuración, validación de posibles vulnerabilidades en componentes de los que dependa (como librerías), manejo apropiado de errores y uso de características de seguridad como minimización de byte-code y protección de la pila de ejecución.

8. Resiliencia a ingeniería reversa. Las recomendaciones agrupadas en esta categoría proporcionan protección contra las consecuencias potenciales de la aplicación de ingeniería reversa, en particular, modificación del código y reempaquetamiento de la aplicación para obtener acceso no autorizado a información sensible. Estas recomendaciones incluyen detección y respuesta a técnicas de análisis dinámico, identificación y acoplamiento con un dispositivo y uso de técnicas de ofuscación.

Implementar estas recomendaciones es inútil si un usuario es víctima de técnicas de ingeniería social y revela sus datos sensibles. Symantec reportó en su informe de 2018 que uno de cada 36 dispositivos en organizaciones presentaba problemas de seguridad porque el usuario había aplicado técnicas para quitar bloqueos de hardware y software (*jailbreak*) o había instalado *malware*. Adicionalmente, las técnicas de suplantación de identidad (*phishing*) siguen siendo ampliamente usadas; un URL de cada 170 involucra esta técnica de ingeniería social[42]. Como consecuencia, es importante que los proveedores de servicios acompañen sus apps financieras con campañas de educación y entrenamiento para el uso seguro de las mismas, informando a los usuarios que la compañía nunca pedirá información sobre inicio de sesión (login) o clave y cumpliendo con este compromiso. Otra forma de atacar este problema es incluyendo cátedras de seguridad de aplicaciones en colegios de educación primaria o secundaria, e incluso en programas universitarios no relacionados con ciencias de la computación.

Conclusiones

Las cifras reportadas por diferentes entidades muestran el alcance actual y potencial de las aplicaciones móviles (apps) y en particular de las apps financieras (fintech) a nivel mundial. Este tipo de aplicaciones ofrece la posibilidad de innovar en diferentes características de los productos o servicios ofrecidos, por ejemplo, atención interactiva al cliente, pagos en línea, finanzas basadas en aspectos diferentes a los tradicionales, reducción de riesgos en finanzas no productivas, finanzas asociadas con la ubicación e independientes de la ubicación, educación financiera e integración de tecnologías emergentes. Colombia no es ajena al desarrollo mundial. El gobierno, las autoridades correspondientes y diferentes entidades apoyan el desarrollo de apps financieras a nivel nacional.

La construcción de las apps financieras presenta retos para todos los participantes en el ecosistema asociado. El gobierno debe entender el funcionamiento del ecosistema y trabajar en una regulación conveniente, que apoye el desarrollo de apps financieras novedosas que responden a necesidades reales y al, mismo tiempo, proteja a los usuarios y sus datos. Los creadores de apps deben identificar necesidades, ser empáticos con los diferentes segmentos de usuarios (incluyendo usuarios con discapacidades), construir un equipo humano adecuado para desarrollar una idea, dar soporte durante todo el ciclo de vida de la aplicación y consultar y responder a la regulación vigente y a sus actualizaciones. Los desarrolladores deben entender todos los requerimientos de calidad, seguridad y privacidad y deben implementar las medidas técnicas necesarias para responder a dichos requerimientos. Además, las organizaciones que distribuyen las apps financieras, desarrolladores, instituciones educativas, y gobiernos, deben considerar el entrenamiento de los usuarios para que ellos manejen su información y las apps de forma apropiada. Solo con la cooperación de todos los participantes en el ecosistema será posible ganar y mantener la confianza de los usuarios y facilitar el desarrollo de este tipo de tecnología.

Referencias

[1] Kyle Taylor, Laura Silver (Pew Research Center), “Smartphone ownership is growing rapidly around the world, but not always equally”, febrero, 2019.

[2] App Annie, “The State of Mobile”, 2019.

[3] Gartner Inc., “Gartner Newsroom Press Releases”, 21 febrero 2019. [En línea]. Disponible: https://www.gartner.com/en/newsroom/press-releases/2019-02-21-gartner-says-global-smartphone-sales-stalled-in-the-fourth-quart. [Último acceso: junio 2019].

[4] Gartner Inc., “Gartner Newsroom Press Releases”, 22 febrero 2018. [En línea]. Disponible: https://www.gartner.com/en/newsroom/press-releases/2018-02-22-gartner-says-worldwide-sales-of-smartphones-recorded-first-ever-decline-during-the-fourth-quarter-of-2017. [Último acceso: junio 2019].

[5] Gartner Inc., “Gartner Newsroom,” 8 abril 2019. [En línea]. Disponible: https://www.gartner.com/en/newsroom/press-releases/2019-04-08-gartner-says-global-device-shipments-will-be-flat-in- . [Último acceso: Junio 2019].

[6] MinTIC, Colombia, “Primera GRAN encuesta TIC/2017. Estudio de acceso, uso y retos de las TIC en Colombia”, 2017.

[7] Departamento Administrativo Nacional de Estadística. (DANE), Censo 2018, 2018.

[8] MinTIC, Colombia, Boletín Trimestral de las TIC - tercer trimestre, 2018.

[9] MinTIC, Colombia, Boletín Trimestral de las TIC - cuarto trimestre, 2017.

[10] App Annie, “2016 Retrospective”, 2016.

[11] App Annie, “2017 Retrospective”, 2017.

[12] Alcaldía Mayor de Bogotá, Guía de sitios Web para las entidades del Distrito Capital, 2017.

[13] Dorfleitner, G., Hornuf, L., Schmitt, M., Weber, M., “Definition of FinTech and Description of the FinTech Industry”, in FinTech in Germany, 2017.

[14] T. Puschmann, “Fintech. Business & Information Systems Engineering”. The International Journal of WIRTSCHAFTSINFORMATIK, 2017.

[15] Merry, Ellen. FEDS Notes, “Mobile Banking: A Closer Look at Survey Measures”, marzo, 2018.

[16] ING, “How do you prefer to pay? Mobile money trends in Europe, the USA and Australia”, julio, 2018.

[17] M. Carney, “The Promise of Fintech - Something New Under the Sun? (Speech given to the Deutsche Bundesbank G20 conference on “Digitising finance, financial inclusion and financial literacy”)”, 25 enero 2017. [En línea]. Disponible: https://www.bankofengland.co.uk/speech/2017/the-promise-of-fintech-something-new-under-the-sun. [Último acceso: junio 2019].

[18] Organisation for Economic Cooperation and Development (OECD), “Financial Markets, Insurance and Private Pensions: Digitalisation and Finance”, 2018.

[19] Murthy Gayatri, María Fernández-Vidal, Xavier Faz, Rubén Barreto. CGAP, “FinTechs and Financial Inclusion. Looking past the hype and exploring their potential”, 2019.

[20] Banco Interamericano de Desarrollo, Invest, Finnovista, “FinTech América Latina 2018. Crecimiento y consolidación”, 2018.

[21] Linares-Vásquez, M., Holtzhauer, A., Bernal-Cárdenas, C., Poshyvanyk, D., “Revisiting Android reuse studies in the context of code obfuscation and library usages”, de 11th Working Conference on Mining Software Repositories (MSR 2014), 2014.

[22] P. Traynor, K. Butler, J. Bowers and B. Reaves, “FinTechSec: Addressing the Security Challenges of Digital Financial Services”, IEEE Security and Privacy, vol. septiembre/octubre, 2017.

[23] R. Schwarz, P. Duston, J. Steele and N. To, The Android Developer’s Cookbook: building applications with the Android SDK, Pearson Education, 2013.

[24] Y. Tian, M. Nagappan, D. Lo and A. E. Hassan, “What are the characteristics of high-rated apps? A case study on free Android Applications”, in IEEE International Conference on Software Maintenance and Evolution (ICSME), 2015.

[25] Linares-Vásquez, M., Bavota, G., Bernal-Cárdenas,C., Di Penta, M., Oliveto, R., Poshyvanyk, D., “API change and fault proneness: a threat to the success of Android apps”, in Proceedings of the 2013 9th Joint Meeting on Foundations of Software Engineering (ESEC/FSE 2013), 2013.

[26] A. Mazuera-Rozo, J. Bautista-Mora, M. Linares-Vásquez, S. Rueda and G. Bavota, “The Android OS Stack and its Vulnerabilities, An Empirical Study”, Emprirical Software Engineering, 2019.

[27] World Health Organization, “World report on disability”, 2011.

[28] Cornell University, “Disability statistics”, [En línea]. Disponible: http://www.disabilitystatistics.org/. [Último acceso: Junio 2019].

[29] Linares-Vásquez, M., Kevin Moran, K., Poshyvanyk, D., “Continuous, Evolutionary and Large-Scale: A New Perspective for Automated Mobile App Testing”, de IEEE International Conference on Software Maintenance and Evolution (ICSME), 2017.

[30] G. Developers, “Android Distribution Dashboard”, [En línea]. Disponible: https://developer.android.com/about/dashboards. [Último acceso: junio 2019].

[31] Ivo Jenik, Kate Lauer. CGAP., “Regulatory Sandboxes and Financial Inclusion”, 2017.

[32] European Securities and Markets Authority, European Banking Authority and European Insurance and Occupational Pensions Authority, “FinTech: regulatory sandboxes and innovation hubs”, 2018.

[33] Diego Herrera, Sonia Vadillo. Banco Interamericano de Desarrollo, “Sandbox Regulatorio en América Latina y el Caribe para el ecosistema FinTechy el sistema financiero”, 2018.

[34] CEMLA FinTechRegulatory Aspects Working Group (REG WG), "Key Aspects around Financial Technologies and Regulation Policy Report", 2019.

[35] Superintendencia Financiera de Colombia, "innovasfc". [En línea]. Disponible: https://www.superfinanciera.gov.co/publicacion/10097165. [Último acceso: junio 2019].

[36] Asobancaria, Segmento Fintech en Colombia: ¿en qué vamos?, 2018.

[37] Symantec Corporation, "Internet Security Threat Report", abril 2016.

[38] L. V. Morales y S. Rueda, "Identifying Android *Malware* Instructions", de IEEE Latin-America Conference on Communications (LATICOM), 2014.

[39] L. M. Jiménez y S. Rueda, "Asegurando Interacciones de Aplicaciones Android", de 10 Conferencia Colombiana de Computación (CCC), 2015.

[40] Sven Schleier y Jeroen Willemsen (Open Web Application Security Project, OWASP), Mobile Appsec Verification, version 1.1, julio 2019.

[41] Open Web Application Security Project (OWASP), "Technical Risks of Reverse Engineering and Unauthorized Code Modification", [En línea]. Disponible: https://www.owasp.org/index.php/Technical_Risks_of_Reverse_Engineering_and_Unauthorized_Code_Modification. [Último acceso: junio 2019].

[42] Symantec Corporation, "Internet Security Threat Report", febrero 2019.

[43] Apple Inc., "App Review," [En línea]. Disponible: https://developer.apple.com/app-store/review/. [Último acceso: junio 2019].

[44] Portafolio, "Número de celulares inteligentes en el país aumentó 50% en el último año", 17 mayo 2017. [En línea]. Disponible: https://www.portafolio.co/tendencias/tenencia-de-smartphones-aumento-50-en-colombia-en-el-2016-505967. [Último acceso: junio 2019].

Reflexiones y buenas prácticas en torno a la investigación del delito informático en Colombia

Armando Colmenares Duque

Introducción

El delito informático actualmente es la conducta delictiva de más crecimiento en Colombia. A diez años de la expedición de la Ley 1273 de 2009, se reciben miles de denuncias por año, especialmente de hurtos por medios informáticos y transferencias no consentidas de activos. Si esta tendencia continúa, pronto será necesario tomar medidas para evitar el colapso de los despachos asignados a estas investigaciones. Como respuesta, por un lado, se han formulado trabajos académicos que intentan analizar la raíz del problema y, por otro, instituciones como la Fiscalía General de la Nación (FGN) han puesto en marcha políticas y mejoras a procesos y metodologías con el fin de atenuar los graves efectos de este tipo de criminalidad. Este trabajo recoge algunas de esas experiencias y sus resultados en la investigación de casos reales asignados a despachos de diferentes partes del país. La divulgación de estas buenas prácticas y sus efectos en procesos judiciales son de gran utilidad para la investigación de futuras causas penales; abriendo la puerta para la reflexión de reformas y repensar la manera como se abordan este tipo de procesos en despachos fiscales a lo largo de todo el país.

El cambio de hitos investigativos

Una de las mayores dificultades identificadas por investigadores judiciales y fiscales en la investigación del delito informático está relacionada con la imposibilidad de formular un plan metodológico de la misma forma como se hace en los demás delitos. A diferencia de otras conductas penales más arraigadas en el día a día de los operadores judiciales, el delito informático se ha separado progresivamente de hitos claves en la investigación, como el lugar de los hechos o la reconstrucción de la línea de tiempo.

Si bien es cierto, toda conducta es relacionable en principio a cualquiera de estas variables, este tipo de criminalidad, por su naturaleza digital, no responde a las mismas lógicas espaciales o temporales y su comprensión resulta contraintuitiva a la praxis generalizada de los investigadores criminales. Esta circunstancia se hizo presente hacia el año 2015, cuando se presentó un aumento de fraudes bancarios que involucraban la inutilización de la tarjeta SIM de las víctimas.

Dado que muchos bancos en Colombia optaron por implementar sistemas de doble verificación en sus sistemas de banca virtual, era común que se enviaran a los celulares de los clientes códigos de cuatro dígitos a través de mensajes SMS, para luego ser usados en el proceso de inicio de sesión (login) del sistema. Rápidamente fue evidente que, sin la obtención de este segundo dígito aleatorio generado por el sistema del banco, eran imposibles las transferencias y avances en las cuentas de la víctima.

Como medida de evasión, hacia finales de 2016 se pudo detectar que previo al fraude, los denunciantes reportaban una perdida permanente de su servicio de telefonía celular. En conjunto con las compañías

celulares de estableció que, con la finalidad de acceder al segundo código de verificación, algunos delincuentes se hacían pasar por sus víctimas ante las compañías de telefonía celular y solicitaban el cambio de tarjeta SIM por motivos de pérdida o daño; un proceso que en Colombia se caracteriza por ser expedito y económico con la finalidad de poder restablecer lo más rápido posible las comunicaciones de un usuario.

Una vez emitida una nueva tarjeta, el delincuente recibía de forma directa los mensajes SMS con destino a la víctima, lo que le permitía cumplir con los pasos de doble verificación dentro del sistema. Este tipo de casos se presentó con cierta insistencia hacia inicios de 2017, lo que llevó a analizar y tratar de asociar los casos bajo una sola línea investigativa con la finalidad de hacer avances rápidos en la identificación de las personas involucradas.

Sin embargo, después de varios meses de indagaciones, los avances eran realmente escasos. La identidad de los autores del delito o el destino final de los dineros hurtados seguían siendo un misterio. Después de meses de trabajo con los investigadores y fiscales del caso se pudo establecer que las dificultades se debían a la aplicación de un enfoque tradicional a la investigación de delitos poco convencionales como los cibernéticos. A pesar de la abundancia de evidencia digital que seguramente reposaba en las plataformas de los bancos, las primeras tareas se orientaron a la recolección de testimonios y entrevistas de las víctimas, que además de ser bastantes, resultaron poco útiles debido a que todas tenían un conocimiento limitado de la forma como habían acaecido los hechos.

A diferencia de un hurto convencional donde las entrevistas de testigos pueden ayudar a describir circunstancias como la hora de los hechos, las características físicas de personas involucradas y modus operandi, en este caso particular después de más de 100 entrevistas realizadas, solo se contaba aún con la información inicial con la que había partido el caso.

Con la finalidad de entender qué técnicas de investigación son útiles, es importante recordar que el delito informático como fenómeno criminal se caracteriza por:

Gozar de separación espacial entre el autor y la víctima. La naturaleza digital de las conductas investigadas hace difícil determinar un espacio físico donde se desarrollan los hechos. El concepto de escena del delito tradicional ha desaparecido para ser ahora considerado una escena digital que puede ser un conjunto de elementos que incluyen diferentes sistemas informáticos de terceros, servidores, redes y demás componentes intangibles que, a pesar de albergar evidencia relevante, no se pueden considerar por sí mismos un espacio físico sobre el cual se puede acceder materialmente.

La identificación de estos lugares digitales y la consideración de la información que pueden proveer a la investigación son claves en la planeación inicial del caso, ya que garantizan la recolección de datos relevantes que por su volatilidad (evidencia digital) pueden perderse o alterarse fácilmente, por lo que su adquisición bajo los procedimientos forenses correctos deben ser una prioridad en todo momento.

Extensión de la línea de tiempo. Los actos ejecutorios de un delito informático son más complejos que los de un delito ordinario. Principalmente porque las fases previas a un ataque informático se relacionan casi exclusivamente con la recolección de información de la víctima, sea esta nombres de usuario, claves personales, hábitos de compra, correos electrónicos, patrones de conducta en la web, etc. Este tipo de datos suelen ser recolectados y clasificados en bases de datos para luego ser usados en ataques coordinados.

Rara vez los ataques son particulares y secuenciales, en cambio se ha podido ver que la mayoría de los hurtos y fraudes relacionados con plataformas bancarias involucran a grupos de clientes con características similares. Dadas estas circunstancias, es difícil plantear como metodología de investigación el reconstruir el histórico de compras del cliente con la tarjeta afectada de las últimas 24 o 48 horas; ya que es muy probable que la recolección de sus datos exceda por mucho el rango de tiempo planteado en la investigación.

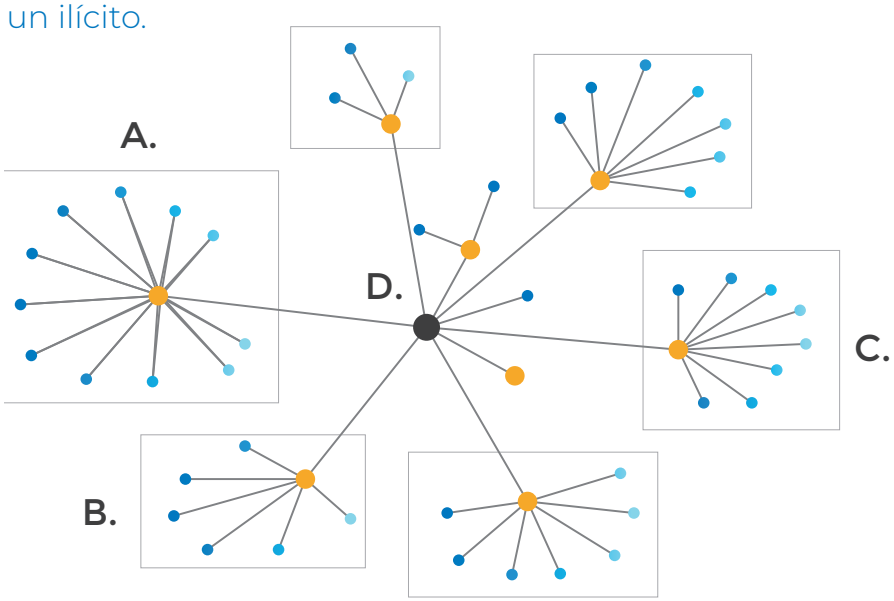
De otro lado, es importante también señalar la gran capacidad de automatismo involucrado en este tipo de tareas. Los ataques informáticos suelen plantearse a gran escala bajo la consideración del alto número de fallos relacionados con el cambio de información periódica del cliente, las actualizaciones de seguridad de los sistemas o el cambio de tecnologías. La imposibilidad de ejecutar individualmente estas tareas deviene en la ejecución automática de estos procesos por miles a la vez en momentos previamente establecidos. Esto separa temporalmente al autor del hecho, que fácilmente podría estar físicamente en otro lugar, imposibilitando construir una relación directa entre el ataque y el atacante.

Estructura organizada por mercados. Uno de los mayores éxitos de la cibercriminalidad está en su estructura altamente especializada. Dada la complejidad de la puesta en marcha de un ataque informático, es cada vez más fácil ver mercados especializados en cada una de las fases, sin que estos tengan necesariamente una relación directa como una sola organización criminal.

En lugar de aglutinarse en una sola estructura jerárquica, como en formas de criminalidad más tradicionales como los carteles y bandas criminales, se han detectado grupos dedicados exclusivamente a actividades como la recolección y compilación de bases de datos con datos personales, otras dedicadas a la falsificación de tarjetas bancarias o al envío de software malicioso a correos personales.

Este tipo de configuración no solo hace más difícil la investigación de una conducta particular, ya que estamos hablando del concurso de varias organizaciones, sino también circunstancias particulares en la investigación de cada una de ellas. A manera de ejemplo, se han investigado un sinnúmero de grupos de mulas de dinero (money mules) que se han especializado en la apertura de cuentas de ahorro con la finalidad de recibir transacciones fraudulentas de dinero.

Figura 1. La estructura representa diferentes organizaciones vinculadas a la comisión de un ilícito.



Si bien D articula los demás grupos, cada uno funciona de forma independiente y se especializa en un mercado criminal específico. La investigación de D difícilmente llevará A, B y C si no se aplican las técnicas adecuadas.

Su investigación pasó por la identificación de cada una de estas personas y el patrón de conducta del grupo. Este caso, que tal vez es la excepción a la regla espacial antes desarrollada, dio frutos cuando se logró la individualización del reclutador, o sujeto encargado de la búsqueda de personas para la apertura de cuentas. Después de seguimientos y agencias encubiertas se logró detener en flagrancia a más de 15 individuos relacionados con cobros de dineros hurtados a cuentas de más de 80 clientes de diferentes bancos.

Circunstancia diferente fue la investigación del origen de los datos usados para los ataques a las víctimas del mismo caso. A pesar de que habían sido detenidos los reclutadores, ninguno de ellos conocía el origen de los datos o quién había efectuado el ataque, ya que su función se suscribía exclusivamente al retiro en efectivo de los activos robados. La identificación de los proveedores de este tipo de datos tuvo que pasar por una búsqueda en la web de grupos en redes sociales dedicados a la venta de bases de datos.

Seis meses después del primer operativo, los peritos informáticos habían identificado al menos tres perfiles de Facebook dedicados a la compraventa de datos personales de clientes de dos instituciones financieras; lo que devino en la compra controlada de dicha información, validando que su contenido era verdadero. Aunque esto llevó a dos capturas más, nunca se pudo establecer la conexión entre los cobradores originalmente aprehendidos y los vendedores de data robada.

Como se puede evidenciar, las técnicas de investigación aplicadas a cada grupo fueron distintas. El acercamiento a cada grupo partió de la consideración de sus características esenciales, permitiendo entablar comunicación con cada una de ellas. Este tipo de análisis es imperativo para plantear la estrategia de investigación criminal. Cada mercado tiene dinámicas diferentes y la identificación de estas antes de iniciar las actividades de judicialización aumenta las probabilidades de éxito de forma notoria.

Alta cooperatividad y baja fricción. Muy diferente a la idea generalizada, el delincuente informático promedio dista mucho de ser un sujeto aislado motivado exclusivamente por el ego o el reconocimiento de sus pares. Si bien muchos de los antecedentes históricos de estos delitos se remontan a este tipo de perfil, lo cierto es que la tendencia actual es a la comisión de fraudes y acceso a sistemas de forma intrusiva motivada enteramente por fines económicos.

Actualmente los fraudes bancarios son llevados a cabo por estructuras organizadas (aunque no jerárquicas) altamente especializadas. Aunque tradicionalmente en cualquier mercado criminal, los grupos participantes compiten por el control del mercado a través de herramientas como la violencia, en el caso del delito informático se ha evidenciado una variación radical de este tipo de comportamiento.

En lugar de ello se han mostrado tremendamente cooperativos, facilitando la labor de otros grupos en el ciberespacio. Un rastreo de foros realizado por policías judiciales en 2016 reveló que muchas de las vulnerabilidades detectadas a sistemas y plataformas bancarias eran hechas públicas, disponibles para cualquier participante de forma gratuita. Esta práctica se extendió también al uso de software malicioso (*malware*), venta de *hardware* intrusivo como registradores de teclas (keyloggers) físicos o piñas Wifi, usadas para el despliegue de varios ataques informáticos.

Si bien podría parecer una práctica contraria a la lógica común, es este punto en particular lo que ha permitido el incremento de las tasas de afectación a los sistemas bancarios. Hay que considerar que el delito informático tiene un costo de introducción bastante alto considerando las habilidades técnicas necesarias para ejecutar un ataque y la gran cantidad de datos de un sistema necesarios para decidir qué tipo de ataque puede llegar a ser efectivo. La impresionante cantidad de información y de materiales disponibles en medios abiertos para realizar un ataque han bajado considerablemente los costos de transacción de cada operación, haciéndolas más fáciles de ejecutar y permitiendo al mismo tiempo probar su efectividad. Como resultado de lo anterior, se eliminó el requisito técnico del delito y permitió el ingreso de sujetos menos capacitados, pero altamente motivados.

En este mismo escenario se desarrolló también el crimen como servicio (crime as a service) en el mercado cibercriminal. En lugar de elegir blancos específicos, algunos grupos criminales se han especializado en la estructuración de sistemas y redes con la finalidad de ser alquiladas con fines delictivos. Sin mucho esfuerzo en la Deep Web se puede alquilar una red de robots informáticos (botnet) ya estructurada con la finalidad de realizar un ataque de denegación de servicio (DDOS) o mejor aún, se puede pagar para que un tercero lo realice.

En estos casos la investigación se ha tornado particularmente compleja; en especial si se tiene en cuenta que la evidencia digital no relaciona directamente a quién ordenó la conducta, solo al ejecutor. Esto suele ser evidente solo después de haber invertido una gran cantidad de recursos técnicos en la recolección de evidencia en sistemas de terceros, usualmente con el uso de mecanismos de asistencia internacional entre países que suelen durar meses en agotarse de forma adecuada.

Sumado a lo anterior, vale la pena destacar que en este proceso no se ejerce la violencia. Dado que el mercado se comporta de forma abierta y cooperativa, no hay grupos u organizaciones dedicadas a ejercer la violencia como forma de control. A diferencia de otro tipo de criminalidad organizada como el narcotráfico, donde la violencia juega un rol importante no solo en la distribución del mercado, sino también en la interacción con las autoridades; en este caso en particular los grupos cibercriminales carecen de incentivos para ejercer este tipo de actos.

Si bien se han registrado casos en los que estructuras tradicionales han patrocinado intrusiones informáticas como forma de expansión de su actividad criminal original; lo cierto es que en general, este tipo de grupos se encuentran perfectamente segregados de los demás y su presencia pasa desapercibida frente a los demás. Dado que la violencia suele ser un indicador importante en la percepción de seguridad, resulta muy difícil encontrar estrategias del gobierno nacional o autoridades locales donde el delito informático sea una prioridad.

Incluso trabajando con los gremios más afectados –los bancos–, todavía este tipo de conductas suelen estar relegadas detrás de la investigación de otras, como el fleteo, el robo a blindados o el asalto a corresponsales bancarios. El crecimiento del delito informático se debe, entre otras cuestiones, a que su importancia se comparó en términos de violencia con otros delitos que parecían más urgentes, desencadenando una ausencia de planes de acción desde la vigencia de la Ley 1273 de 2009.

Este problema de concepción sobre la gravedad del delito informático afecta incluso la forma como los jueces analizan los casos. En las medidas de aseguramiento de carácter preventivo es usual que se considere que la prisión domiciliaria es más proporcional que una medida intramural, en especial si se considera la usual ausencia de antecedentes penales de los capturados, la sobrepoblación carcelaria y el análisis de proporcionalidad de los hechos con respecto a otros más gravosos que se presentan a diario en Colombia. Sin embargo, resulta evidente que una medida domiciliaria suele dejar a la mano del sujeto procesado todos los elementos necesarios para continuar ejecutando la conducta.

Las particularidades de la evidencia digital. Una de las brechas más importantes que se han identificado en la investigación del delito informático se refiere a la identificación y recolección de evidencia digital. Ya se ha señalado del fenómeno de la dispersión de la escena digital, que implica la multiplicidad de plataformas involucradas en la prestación de un solo servicio que tiene como resultado la multiplicidad de datos en sistemas de diferentes terceros, usualmente no todos afectados por el fraude y, por ende, menos dispuestos a coadyuvar en la investigación.

En otros casos la ubicación de la data relevante puede estar en otra jurisdicción, lo que dificulta enormemente la recolección de la evidencia y su integración en el proceso penal bajo los criterios de cadena de custodia. En estos casos concretos, es necesario que el fiscal conozca y use con efectividad los canales de cooperación internacional con la finalidad de comisionar a autoridades extranjeras la realización de actos de investigación. Este tipo de herramientas, salvo las dispuestas en la red 7/24 de países suscribientes del convenio de Budapest, suelen ser bastante lentas y estar condicionadas a las regulaciones y políticas de privacidad de cada país.

El procesamiento de grandes cantidades de datos es un reto importante. Actualmente los laboratorios de informática forense de los cuerpos técnicos de investigación en todo el país están saturados de órdenes de trabajo relacionadas con la extracción y conservación de todo tipo de evidencia digital que no está necesariamente ligada a casos donde se investiga la comisión de delitos informáticos. Este aumento progresivo de la necesidad de usar peritos informáticos en la recolección de todo tipo de evidencia digital, procedimiento técnicamente menos complejo, ha dejado menos espacio y tiempo a expertos para el desarrollo de labores forenses más complejas. Casi la totalidad de las horas-hombre de los laboratorios se invierten en las tareas forenses más básicas, dejando poco margen para la realización de labores forenses complejas.

Como resultado de ello se han compilado grandes cantidades de evidencia digital sobre las cuales no se han explotado las fases de análisis a fondo, dejando las investigaciones llenas de datos que aportan realmente muy poca información. Repensar y planear qué tipo de evidencia se requiere recolectar y cómo va a ser usada posteriormente en la verificación de la teoría del caso de la Fiscalía es una prioridad para los operadores judiciales. Cada vez es más común encontrar dispositivos con alta capacidad de almacenamiento, por lo que priorizar las labores de investigación a los datos necesarios es un imperativo.

En enero de 2019 se recibió por primera vez en el laboratorio de informática forense del Cuerpo Técnico de investigación el primer dispositivo celular con una memoria de 1 tera de capacidad. Aunque la extracción de la información le ocupó al equipo forense unas 6 horas de análisis, tomará al menos 50 horas a un investigador revisar el contenido de la imagen que se obtenga. Si la tendencia continúa, pronto la gran cantidad de datos saturarán las capacidades humanas y técnicas de los cuerpos de investigación.

La presentación de resultados ante el estrado judicial es un reto sobre el cual se está trabajando. Debido a la complejidad técnica del proceso de extracción y fijación, es común que los fiscales tengan dificultades en la introducción del elemento digital en juicio o no puedan explicar con claridad al juez procedimientos forenses sobre los cuales la defensa formule objeciones. La audiencia preparatoria suele ser un espacio usado comúnmente por las bancadas defensivas para atacar la viabilidad probatoria del elemento que se pretende introducir en el futuro juicio. En este espacio, muchas veces se llevan a cabo discusiones técnicas ampliamente resueltas por la gran mayoría de protocolos forenses del mundo, que al no ser conocidos por las partes y principalmente por el juez, dilatan y entorpecen la dinámica de la audiencia.

Uno de estos casos se presenta cuando se ataca algunas funciones hash específicas como el MD5, dado que es posible que esta pueda producir la misma secuencia alfanumérica de identificación a dos piezas

de información digital totalmente diferentes. Aunque está probado que estadísticamente es altamente improbable, matemáticamente es posible, por lo que en ocasiones este argumento se ha utilizado para cuestionar la validez de esta técnica para conservar y fijar la evidencia digital. Aunque los protocolos de informática forense dictan que esta dificultad puede ser fácilmente sorteada extrayendo dos secuencias alfanuméricas de dos funciones hash distintas (MD5 y SHA1, por poner un ejemplo), es común que una vez planteada la duda por la defensa, el fiscal tenga que solicitar un aplazamiento para consultar con sus técnicos este tipo de objeciones.

Aunque el rol del fiscal no se extiende a conocer a profundidad el alcance de las técnicas forenses aplicadas a la evidencia del caso, si se requiere la socialización de conocimientos básicos sobre evidencia digital, su proceso de conservación y la fiabilidad de las técnicas mediante las cuales se recolecta y conserva la evidencia. Un proceso similar al que se agotó décadas atrás cuando se introdujo el ADN como evidencia demostrativa en las investigaciones judiciales.

La tecnología como una práctica riesgosa. El fenómeno de la hiperconectividad cambió para siempre la relación de los humanos con la tecnología y el mundo que los rodea. Con una suscripción de cuenta de correo se pueden sincronizar datos como los contactos, geolocalización, galerías multimedia, documentos de trabajo, redes sociales, datos personales, claves de acceso a plataformas, calendarios, espacios de almacenamiento en la nube, cuentas de aplicaciones, chats, entre otros. A pesar de que este tipo de sistemas fueron diseñados en virtud de la convergencia de servicios en un solo dispositivo, nunca se había concentrado tanta información sensible en un solo lugar.

Esto contrasta con la poca conciencia que existe entre los usuarios digitales en valorar su nivel de exposición, comprender el valor de sus datos y tomar medidas de seguridad informática que proteja su privacidad. Esta es una marcada diferencia que tiene el delito informático con otros delitos investigados por la FGN. Cuando se trata de conductas de alto impacto como hurtos, lesiones personales e incluso estafas, la primera línea de defensa suelen ser las medidas de autocuidado que la víctima despliega sobre sí.

Decisiones básicas como no transitar por calles oscuras o evitar sitios ampliamente reconocidos como peligrosos suelen ser medidas de prevención populares que mantienen alejada a la víctima de posibles agresores. En contraste, estas mismas personas suelen adoptar comportamientos bastante riesgosos en la web cuando se trata de sus datos personales. A cambio de contenido en línea como series y películas, se entregan correos electrónicos, datos de contacto y nombres reales. Esto, sumado a la arraigada práctica de consumir software no licenciado, deja a la víctima en una condición de vulnerabilidad a la hora de acceder en el mismo equipo al sistema web de su banco.

Estas acciones que suelen ser a propio riesgo, teniendo en cuenta que son ampliamente socializadas por proveedores de software y expertos en seguridad informática, suele ser la vulnerabilidad más explotada por los atacantes informáticos. Este problema no se limita solo a personas individualmente consideradas; el sector corporativo también suele tener dificultades en la implementación de políticas ciberseguras, en especial las relacionadas con la protección de los datos personales de sus clientes y empleados.

En este aspecto, las compañías todavía ven la seguridad informática como un gasto y no como una inversión. Por lo que sus redes y sistemas son muy básicos y los datos más sensibles suelen estar expuestos no solo a atacantes externos, sino a disposición de personas con acceso a información privilegiada (insiders) dispuestos a venderlos a la competencia o a usarlos en beneficio propio en la comisión de fraudes. Investigaciones penales donde las empresas han denunciado acciones intrusivas en sus sistemas y servidores han demostrado que el origen suele ser un empleado descontento o con privilegios desproporcionados en los aplicativos corporativos.

Portalmotivo,lasectorizacióndelasredes,laauditoríadeperfilesyactividades,asícomolacompartimentación de la información sensible suele ser muy importante en la prevención e incluso la investigación de delitos informáticos. En empresas con políticas de datos maduras, las auditorías regulares de sus sistemas suelen detectar con mayor prontitud las deficiencias de sus procesos y los posibles fraudes internos de las que son objeto. Esta labor también ayuda a las autoridades a recolectar evidencia de forma precisa y documentar normativamente las políticas y regulaciones internas eventualmente violadas por empleados y visitantes. Esto permite construir, desde el punto de vista penal, elementos como el conocimiento de la antijuricidad de la acción cometida.

Consideraciones económicas de la cibercriminalidad

El análisis económico del delito es una herramienta ampliamente usada en la proposición de políticas públicas encaminadas a la mitigación y prevención de todo tipo de conductas punibles. Aunque tiene limitaciones en razón a los presupuestos que usa, especialmente el concepto de racionalidad, para el caso concreto suele ser muy útil debido a la alta concentración de delitos relacionados con fraude bancario, lo que ayuda a valorar de mejor forma los costos y beneficios del actuar criminal.

Como punto de partida es muy útil partir del concepto de racionalidad aplicado a la criminalidad, tratado con amplitud en 1974 por Gary Becker en su trabajo “Crime and Punishment” donde plantea, a partir del análisis de algunos delitos ampliamente denunciados (ninguno de ellos informático), que el crimen puede ser valorado como un mercado, asignándole al delincuente una lógica racional mediante la cual una conducta punible solo es cometida si los beneficios de realizarla exceden los costos de ejecutarla.

Dejando de lado algunas teorías criminológicas como el comportamiento impulsivo o condicionantes biológicos, las condiciones socioeconómicas como aspecto subyacente a la predisposición criminal o las tesis relacionadas con el delito altruista, Becker se centra en el análisis de la probabilidad de ser atrapado como una variable empíricamente relacionada con la cantidad de delitos cometidos. La variación de esta probabilidad tiene una relación directa con la oferta de delitos en el mercado criminal y por ende representa un punto de partida para la formulación de una política criminal.

La premisa aplicada consiste entonces en plantear que un delincuente cometerá un delito solo si los beneficios resultantes del mismo exceden el costo de ejecutarlo o el beneficio esperado si se dedicara a otra actividad no criminal (costo de oportunidad). La relación entre el número de delitos y la probabilidad de ser atrapado puede representarse a través de una función de la forma:

$$O_j = O_j (P_j , F_j , U_j)$$

Donde Oj es el número de delitos cometidos durante un periodo específico, Pj la probabilidad de condena por cada delito cometido, Fj el castigo establecido por cada delito y Uj representa la sumatoria de otras variables que coadyuvan o disuaden al individuo a tomar la decisión cuando analiza el costo de su acción, tal como el estigma social y moral de cometer un delito o el prestigio y fama en el mundo criminal por completar una acción de tal tipo.

Dado que solo los delincuentes son condenados, pero no todos los delincuentes lo son, encuentra Becker que existe una discriminación de precios y una incertidumbre al momento de tomar la decisión. Como resultado, un aumento de Fj o Pj reduciría la utilidad esperada de cada delito, lo que terminaría por disminuir la cantidad de Oj. Esta relación es descrita de la forma:

$$O_{pj} = \frac{\delta Oj}{\delta Pj} < 0 \qquad O_{fj} = \frac{\delta Oj}{\delta Fj} < 0$$

La variación de Uj también tiene el potencial de afectar la utilidad esperada. Becker explica que un incremento del respeto a las normas y leyes como resultado de la educación o la influencia de la moral puede reducir los incentivos de cometer un delito y, por ende, reducir el número total de conductas cometidas Oj.

Otra interesante relación se encuentra en las variaciones de Fj y Pj y su efecto en Oj. Un aumento de Pj compensado por una disminución de Fj no varía el beneficio de un delito; sin embargo, si afecta la utilidad esperada ya que esto representa una variación del riesgo. Bajo esta lógica, un aumento de Pj reduciría la utilidad esperada y por ende el número total de delitos cometidos Oj. Así mismo, si j es averso al riesgo, un incremento solo de Fj que no varíe Pj tendría un efecto neutro sobre el conteo total de delitos cometidos.

Finalmente, teniendo en cuenta que J, como sujeto individualmente considerado, está sometido a otras variables que pueden afectar, especialmente Uj, Becker señala que la función simplificada más adecuada es aquella que se representa bajo la forma:

$$O=O(p,f,u)$$

Donde la relación entre el total de delitos cometidos depende de la probabilidad de ser condenado, el castigo total por el delito cometido y la consideración de otras variables subjetivas en torno al sujeto y la conducta que realiza. El aumento del total de castigo por conducta tiene poco efecto si la probabilidad de condena se mantiene constante; pero el aumento de las probabilidades de ser condenado excluye del total de delitos cometidos a aquellos criminales que sean aversos al riesgo, dejando solo aquellos dispuestos a asumir dentro del costo de la acción la probabilidad de ser condenados.

Un enfoque similar aplicado al delito informático planteó Nir Kshetri en el trabajo de 2006 *"The simple economics of cybercrime"*, en el que extiende el modelo de Becker en una función costo beneficio de la forma:

$$M_b + P_b > O_{cm} + P_a\ P_c$$

Donde Mb es el beneficio monetario de cometer el delito, Pb representa el beneficio psicológico del delito, Ocm es igual al costo de oportunidad monetario de ser condenado, Ocp el costo psicológico de cometer el delito, Pa la probabilidad de ser arrestado y Pc la probabilidad de ser condenado. El producto total de Ocm Pa Pc es denominado efectos esperados de la sanción. Si los beneficios esperados superan los costos esperados, el delincuente encontrará racional ejecutar el delito.

En consideración de lo anterior, varias conclusiones se pueden plantear a la hora de formular política criminal relacionada con el delito informático en general:

En primer lugar, la cantidad total de delitos está supeditada por un conjunto de condiciones y supuestos que le hacen a un sujeto racional más beneficioso cometer un delito que abstenerse de ello. Siempre que el beneficio de un delito sea mayor que su costo, habrá un incremento del total de delitos cometidos, por lo que cualquier política orientada a disminuir el delito cibernético deberá estar diseñada para identificar los beneficios con el fin de disminuirlos y aumentar los costos con la finalidad de reducir los incentivos.

El costo del delito está compuesto por el costo de ser condenado, que se podría equiparar para fines de análisis de este trabajo a la pena imponible para cada delito tipificado, y la probabilidad de ser condenado, que a su vez en el modelo de Kshetri es divido en dos (costo de ser atrapado y costo de ser condenado). El aumento del costo del delito o la probabilidad de ser condenado afectan el total de delitos cometidos. Sin embargo, el aumento del costo del delito por si solo sin una variación de la probabilidad de ser atrapado tiene poca incidencia en la reducción del total de delitos cometidos dado que, si el riesgo inicialmente considerado se mantiene, incluso los agentes aversos al riesgo estarán dispuestos a asumir el costo final del delito cometido.

De otro lado, si las probabilidades de ser atrapado incrementan, esto tendrá una incidencia mayor en la cantidad de delitos debido a que con altas probabilidades de ser condenado, la utilidad esperada puede disminuir de forma drástica para el agente, por lo que bajo estas condiciones solo aquellos que tomen decisiones riesgosas seguirán adelante.

Otro elemento importante es la diferenciación entre las posibilidades de ser atrapado y las de ser condenado. Esto separa claramente dos fases procesales en el procedimiento penal que presentan escollos probatorios para fiscales e investigadores. El primero tiene que ver con la identificación y ubicación del autor de un delito informático. Entre el 60% y 80% de las investigaciones archivadas por delitos informáticos están relacionadas con la imposibilidad de encontrar el sujeto activo de las conductas investigadas. Sea por la imposibilidad de rastrear una IP debido al uso de servidores y proxys en el extranjero o el uso de servicios comerciales que no requieren de validación de identidad con el fin de proveer anonimato a sus clientes, la identificación del autor material de la conducta es uno de los retos más importantes de una investigación. De otro lado, la ubicación y arresto del probable autor de una conducta no es el único problema. Pasada la fase preliminar de la investigación es necesario construir un caso que pruebe más allá de toda duda razonable la ocurrencia de un delito y la participación del investigado en los hechos.

Esto implica la correcta planeación de la investigación donde se recolectaron todos los elementos materiales probatorios necesarios para la prueba del hecho y la participación del autor, en cumplimiento de los parámetros legales y forenses en el tiempo establecido para evitar la pérdida de datos o su modificación; todo respetando la cadena de custodia y las garantías constitucionales concernientes con el derecho a la intimidad y la protección de datos del indiciado o terceros.

Políticas orientadas a aumentar la probabilidad de ser atrapado

La información asimétrica en el mercado de la ciberseguridad. La ausencia de información exacta relacionada con incidentes informáticos representa una dificultad enorme a la hora de cuantificar y analizar el estado de la ciberseguridad en Colombia. Parte del problema está representado en la ausencia de coordinación entre entidades estatales y privadas en la centralización de datos y su correcta categorización.

Solo en Colombia, la Fiscalía General de la Nación, la Policía Nacional y algunos observatorios gubernamentales se dedican de forma independiente a la recolección de información relacionada con delitos informáticos. En muchos casos, los datos se recogen bajo metodologías y categorías distintas, haciendo imposible una depuración de estos. Mientras la FGN tiene reportes de denuncias por cada delito de la Ley 1273 de 2009, la Policía Nacional ha optado por un enfoque más amplio, contabilizando en sus estadísticas denuncias por tipo de ataque, midiendo fenómenos como el suplantación en móviles (smishing), suplantación en voz (vishing) o suplantación de identidad (*phishing*).

Paralelamente se contabilizan por entidades estatales estadísticas relacionadas con incidentes informáticos. Los incidentes en infraestructuras críticas son recolectados por el Comando Conjunto Cibernético y los relacionados con entidades públicas o privadas de interés son, a su vez, contabilizados por el ColCERT. Cada uno de estos equipos compila datos de incidentes informáticos que en pocas ocasiones son considerados como delitos. En esta misma línea los gremios afectados por fraudes, especialmente el bancario, han optado por asumir de forma colectiva la gestión de incidentes a través de la configuración de CSIRT. Este tipo de equipos suelen poseer datos de tendencias y frecuencias de ataques de la industria; información muy valiosa que no se transmite ni a los CERT de gobierno ni a las autoridades dedicadas a la investigación judicial.

Por otro lado, las víctimas en este tipo de delitos suelen tener un promedio de denuncias más bajo que otros delitos de alto impacto. A pesar de que el crecimiento de las denuncias por delitos informáticos ha crecido de forma constante desde 2009, la cifra negra de conductas que no se denuncian también es bastante alta, lo que aleja una porción del universo de casos investigables fuera del espectro de las autoridades.

La ausencia de información exacta sobre el nivel real de delitos y el estado de seguridad del ecosistema web de Colombia hace que el mercado de la ciberseguridad se comporte como un mercado de 'limones', tal y como fue descrito por Akerlof en 1970. Al no haber claridad sobre la condición real del delito informático y su afectación a usuarios bancarios, el mercado no genera suficientes incentivos relacionados con la provisión de soluciones en ciberseguridad y ciberdefensa. En Colombia las instituciones públicas dedicadas a esta tarea iniciaron labores solo después de la suscripción de dos documentos CONPES.

En el caso de las instituciones financieras, los incidentes informáticos registrados, así como los fraudes bancarios sufridos por sus víctimas, son investigados y asumidos como parte del riesgo operacional. Aunque este enfoque ha demostrado en Colombia no haber dejado de lado las garantías y obligaciones que el sector tiene con sus clientes, sí es incierta la sostenibilidad de esta política a largo plazo. Mientras el mercado no ajuste los precios de acuerdo con las condiciones reales de la ciberseguridad, los bancos estarán menos motivados a invertir en soluciones abiertamente pensadas para hacer menos riesgosas las transacciones bancarias dado que el costo no será asumido por los clientes. Estos a su vez se negarán a pagar precios elevados por canales y sistemas más seguros si no conocen la extensión del riesgo real al que se exponen cuando se realizan transacciones de banca virtual.

La solución a esta dificultad se ha venido gestando en dos ámbitos distintos desde el año 2016. Para el caso del sector público, la existencia de varias agencias dedicadas a la ciberseguridad, ciberdefensa e investigación del delito informático sin una coordinación o intercambio de información ha probado ser la prioridad de los últimos gobiernos; en especial después de la atención de casos donde todas ellas eran competentes para actuar. Esto se dio por primera vez en el marco del referendo por la paz del año 2016 donde se votaron los acuerdos suscritos en La Habana entre el gobierno nacional y las Farc.

Durante el periodo previo a las elecciones la plataforma de la Registraduría Nacional del Estado Civil, que dispone de un módulo de consultas de mesas de votación en su página web, fue objeto de un ataque informático de deformación (defacement) que hacía que la consulta arrojara el resultado "usted está muerto". Dada la importancia de la plataforma en el certamen democrático que se llevaba a cabo, se conformó una mesa de crisis de gobierno que invitó a todas las instituciones a participar. Sin embargo, pronto fue obvio que sobre la mesa había varias prioridades difíciles de armonizar.

Por un lado, la evidente necesidad de mantener funcionando la plataforma y su módulo de consultas movió a técnicos de la Registraduría y el ColCERT a restablecer lo más rápido posible el sistema, uno de los

principios fundantes de un equipo de respuesta cibernética. De otro, entidades como la Fiscalía General de la Nación y la Policía Nacional estaban interesadas en investigar de la forma más rápida posible los hechos para rastrear los autores materiales detrás de estos. La solución a estos inconvenientes requirió de coordinaciones de alto nivel para poder garantizar la toma de decisiones rápidas en el momento preciso.

En las seis horas posteriores al evento, el incidente había sido atendido y en las fases subsiguientes de aseguramiento del sistema se inició la recolección de evidencia digital, lo que permitió que dos días después del ataque se diera la captura del responsable en la ciudad de Medellín. Estas circunstancias dejaron como lección a todos los participantes que la coordinación de incidentes era posible, pero requería de un modelo que considerara las prioridades de todas las instituciones y las gestionara de forma eficiente en las primeras horas de atención al incidente. Así fue como se conformó la mesa para el diseño de Modelo Nacional de Gestión de Incidentes, que tiene como función principal la articulación de las capacidades cibernéticas del Estado colombiano en el marco de un incidente informático.

El modelo actualmente se encuentra aún en discusión debido a las variadas dificultades de carácter legal y gubernativo propias de articular sectores como el de justicia, defensa y seguridad ciudadana. Una de las más importantes tiene que ver con la entrada al sistema a partir de la detección del ataque por parte de SOC privados y públicos o a través de denuncias de la ciudadanía. Considerando el alto número de incidentes presentados a diario, cuál de esa porción debería ser investigada por la Fiscalía.

Otra dificultad está relacionada con la ausencia de funciones de policía judicial de algunas instituciones como el Comando Conjunto Cibernético y, por ende, su incapacidad para la recolección de elementos materiales probatorios durante la atención a un incidente. Este tipo de actos urgentes suelen llevarse a cabo por grupos diferentes de forma posterior a que los equipos de respuesta restablezcan las funciones del sistema, lo que pone en riesgo la volátil evidencia digital disponible para la investigación. Su solución requeriría de unidades interagenciales preparadas para ejecutar ambas labores lo más pronto posible, no solo garantizando la continuidad del servicio sino las probabilidades de éxito de la investigación.

Otro punto de trabajo es la difusión de la información contenida en denuncias que reciben la FGN y la Policía Nacional. Actualmente la información en este tipo de casos no es difundida a otros sectores de gobierno ni entidades bancarias debido a que la fase preliminar de la investigación goza de reserva. Sin embargo, se ha hecho evidente que desde esta etapa ya se pueden perfilar amenazas y vulnerabilidades concretas que están siendo explotadas. La compartimentación de esta información y el uso generalizado de herramientas informáticas en diferentes instituciones financieras prolonga el ataque en diferentes bancos hasta que la vulnerabilidad es ampliamente conocida.

El análisis de la taxonomía del ataque empleado y difusión en la industria afectada es de gran ayuda para prevenir ataques futuros, contener la extensión del daño en otros sistemas y bajar el nivel de entradas al sistema penal acusatorio por denuncias. Como medida preventiva esto no solo coadyuva a prevenir a víctimas de ataques similares, también permite mantener descongestionados los laboratorios forenses y despachos fiscales de causas penales que podían ser evitadas.

Con esta finalidad ya son varias iniciativas que incluyen la redacción de boletines y alertas tempranas que previenen a los equipos de seguridad informática bancaria del país. Inicialmente estas son emitidas por la Policía Nacional y para ataques específicos, el ColCERT. El próximo paso es ampliar la cobertura de estos comunicados, incluyendo información procesada de denuncias por delitos de la Ley 1273 de 2009, que señalen las tendencias mensuales de este tipo de conductas (censo delictual) y la técnica informática específica que tuvo éxito en casos concretos.

La investigación del delito informático como un juego cooperativo. Una particularidad especial de la investigación del delito informático tiene que ver específicamente con la dispersión de la evidencia digital y la concurrencia de varios actores (sistemas informáticos o personas) que deben ser articulados y consultados de forma independiente con el de fin adelantar una investigación judicial.

En marzo de 2017 se abrió una investigación en el CTI de la Fiscalía donde se indagaba por un fraude a seis clientes de una entidad bancaria por una cifra inusualmente alta para un conjunto tan reducido de víctimas. El análisis de las transacciones objetadas arrojó que todos los dineros habían sido transferidos a un fondo de pensiones debido a que las cuentas habían sido usadas para pagar a terceros las cesantías. Como para ese momento era evidente que ninguna de las víctimas era empleadora de los beneficiarios de estos fondos, estaba claro que estos habían participado del fraude prestando sus nombres para las consignaciones objetadas.

Cuando se inició la reconstrucción del caso, se vio claramente que la evidencia se encontraba dispersa en varias entidades que habían participado del proceso de pago y que por tanto tenían una pieza de la transacción en sus sistemas. El banco tenía la información relacionada con los accesos a la plataforma de los clientes, la entidad destinataria, los saldos enviados en cada transacción y las horas exactas del incidente. De otro lado, el fondo de pensiones tenía los datos personales de los beneficiarios y su respectivo historial de crédito en el fondo. También eran los únicos que podían proporcionar cuándo y dónde fueron inscritos los beneficiarios y la empresa a la que supuestamente estaban vinculados laboralmente.

Finalmente, atendiendo a que estos pagos involucraron planillas de liquidación de aportes a seguridad social y un botón de pago, había dos instituciones más que habían mediado para el pago de los aportes entre el banco y el fondo. Debido a los buenos oficios del banco y su área jurídica, se pudo establecer que los dineros no habían sido retirados por los receptores en el fondo de pensiones, lo que daba aún la oportunidad de bloquear estos pagos y reversar la transacción.

El trabajo de la policía judicial se centró entonces en identificar e individualizar cada transacción a través de técnicas forenses y garantizar qué dinero exactamente correspondía a transferencias fraudulentas, para luego rastrearlas desde su punto de inicio (banco) hasta el beneficiario final. La recopilación de esta información tardó meses y requirió de autorizaciones judiciales que en la gran mayoría de casos tuvieron que ser prorrogadas o solicitadas nuevamente por superar los términos legales correspondientes.

Mientras esta fase se agotaba, se desarrolló una estrategia jurídica dedicada a impedir que los dineros fueran cobrados y lograr su devolución a los clientes lo más rápido posible. Esto también requirió la inversión de tiempo del fiscal, los representantes del banco y el fondo en audiencias ante un juez para que de forma provisional se ordenara cautelarmente el congelamiento de los fondos y, posteriormente, su consecutiva devolución.

El éxito de esta investigación obedece a que todas las partes estaban motivadas e hizo que emplearan estrategias comunes que les permitieran a todos la resolución del fraude. Este tipo de escenarios pueden describirse en teoría de juegos como juegos cooperativos, donde cada jugador no compite con los demás debido a que tiene incentivos para desarrollar estrategias comunes dado que todos persiguen el mismo objetivo, por lo que resulta más eficiente plantear coaliciones.

En el ámbito de la ciberseguridad y el delito informático, la cooperación entre los actores vinculados a la investigación es muy importante. Desde el punto de vista judicial, la ayuda mutua entre las partes agiliza los procesos de identificación y análisis de evidencia digital, poniendo a disposición de los peritos informáticos data digital que puede perderse antes que el fiscal sepa que existe y considere necesario su recuperación.

De otro lado, la mejora de los tiempos de investigación no es la única ventaja de las estrategias cooperativas. En el ámbito judicial, muchos bancos han optado por invertir más esfuerzos en impulsar juicios claves en contra de organizaciones criminales o con alto conocimiento técnico dedicados al fraude bancario. Es importante señalar que la investigación es solo la primera fase del caso, pues resta todo el trámite del juicio, que requiere esfuerzo adicional de las partes debido a su complejidad y duración en el tiempo.

Este ejercicio no solo consolida un bloque sólido dentro del proceso entre Fiscalía y víctima; sino que además ha demostrado ser muy útil en regiones del país donde los fiscales que atienden incidentes informáticos tienen poca experiencia en el manejo de la evidencia digital o desconocen la información disponible que puede ser usada para investigar los hechos. En estos casos, la asesoría que brindan los bancos durante todo el proceso es de gran ayuda para estos funcionarios, que al estar asignados por competencia legal a la de otros delitos de impacto como el caso de las lesiones personales, la inasistencia alimentaria y hurtos simples, ven el delito informático con cierta prevención por su alto contenido técnico.

A nivel de gobierno, también ha sido de utilidad la cooperación entre entidades. Entre la Fiscalía General de la Nación y Asobancaria existe una relación de varios años enfocada al mejoramiento de las investigaciones penales por delitos de la Ley 1273 de 2009. Ambas partes se han beneficiado mutuamente; por un lado, la Fiscalía ha tenido acceso a actualizaciones y capacitaciones sobre ciberdelincuencia y Asobancaria ha logrado subir el estándar investigativo de fiscales en regiones donde las tasas de denuncias por hurtos por medios informáticos y transferencias no consentidas de activos han aumentado.

Esta cooperación también se ha extendido a las universidades, que ven en los laboratorios y despachos de la Fiscalía espacios únicos para la investigación académica. Esta relación ha permitido el intercambio de conocimientos en procedimientos forenses y estrategias jurídicas para la legalización de evidencia digital; lo que ha llevado a la introducción de investigaciones académicas al ámbito judicial y ha mejorado ampliamente los protocolos de manejo de evidencia digital y el análisis de resultados periciales.

A este tipo de políticas es necesario aún involucrar otros actores. Otras instituciones de gobierno, como el MinTIC, podrían mejorar procesos como la suspensión de dominios con *phishing* en comunicación con las entidades bancarias y la FGN. La mejora de los canales de comunicación entre bancos e investigadores disminuiría los tiempos de respuesta a requerimientos de información con término legal para su obtención, y el diseño conjunto de protocolos de investigación para las conductas más comunes puede ayudar a mejorar el plan metodológico del caso y, por ende, sus resultados.

Políticas orientadas a aumentar la probabilidad de ser condenado

La aplicación de las técnicas de investigación del crimen organizado al delito informático. Obviando algunos delitos específicos cometidos por organizaciones hacktivistas o hackers solitarios, la gran mayoría de las denuncias por fraude bancario en Colombia están motivados por el lucro que genera esta actividad y normalmente la llevan a cabo estructuras organizadas y especializadas.

Aunque la Ley 1273 de 2009 introdujo un catálogo de delitos relativamente nuevos y con gran complejidad técnica en su investigación, un fiscal puede sacar partido de la aplicación de las técnicas ya aprendidas en la investigación y desarticulación del crimen organizado. Este acercamiento ha demostrado ser altamente efectivo ya que las reglas de organización que rigen en estructuras dedicadas al narcotráfico o similares suelen estar presentes también en grupos de ciberdelincuentes.Aunque con finalidades y dinámicas distintas, todos los grupos pueden describirse a través de roles, funciones y perfiles. El identificar cada una de estas variables en la investigación permite la valoración completa del fenómeno y fortalece la imputación de la FGN, dado que se podrán incluir delitos no informáticos, como el concierto para delinquir, y se podrá

también demostrar la posibilidad de la continuación de la actividad delictiva en la solicitud de una medida de aseguramiento consistente en detención preventiva.

El rol es la función que un individuo particular desempeña en el grupo. Dependiendo de las actividades desempeñadas por la organización habrá distintos roles diseñados para ejecutar una fase específica del proceso. Las funciones son aquellas tareas concretas que debe ejecutar alguien que desempeña un rol específico, y finalmente el perfil, que se define como aquellas características objetivas y subjetivas del sujeto que le permiten asumir un rol para desempeñar ciertas funciones.

A manera de ejemplo, pensemos en una organización dedicada al fraude bancario a través de transacciones a cuentas de terceros. Será necesario que alguien asuma el rol de intruso (intruder) y acceda a la plataforma de banca virtual del cliente e inscriba las cuentas de los beneficiarios de las transacciones irregulares. Para ello, es su función obtener de la red software malicioso capaz de capturar el usuario y la contraseña de la víctima, usarlos para acceder al portal e inscribir las cuentas de otros miembros de la organización. Este rol suele ser ocupado por una persona con conocimientos en seguridad informática, con acceso a foros y bases de datos de *malware* y con experiencia en este tipo de ataques.

Esta técnica de perfilamiento es bastante útil en organizaciones dedicadas al narcotráfico debido a que permite la estructuración de un grupo en función de sus roles, lo que ayuda a orientar la investigación y capturar a los individuos más importantes, logrando así la desarticulación del grupo. Para el caso informático, una vez identificados los miembros de la organización con sus respectivos roles, será evidente que los miembros más especializados y, por consiguiente, menos reemplazables son los que deben ser capturados primero, y así llevar a la banda a su desarticulación efectiva. Otros que ejerzan funciones con roles menos importantes pueden ser fungibles y, por ende, su judicialización no llevará al fin de las actividades, por lo que no pueden ser priorizados en la investigación.

Otro tipo de técnicas como las agencias encubiertas, en especial las virtuales recientemente introducidas a la legislación colombiana, también son muy útiles para investigar grupos. Estas permiten tener contacto de primera mano con los miembros de la organización y conocer las técnicas y dinámicas aplicadas al fraude que se está investigando. Las agencias que se han puesto en práctica hasta la fecha en este campo han resultado además muy eficaces en la recolección de datos informáticos que se solían desconocer en otras investigaciones. En 2018, una investigación en Bogotá logró conocer a través de la actuación de un agente encubierto la existencia de grupos dentro de establecimientos de cadena que copiaban los datos de las tarjetas de crédito de los clientes mientras se hacia el pago.

Este grupo compilaba y vendía la información a terceros que la usaban para hacer grandes compras de electrodomésticos en otros establecimientos de comercio. Con el tiempo el agente llegó a conocer ambas estructuras, en principio distintas, que no hubiese sido posible investigar de otra forma debido a la ausencia de otras evidencias igual de eficaces.

Finalmente, el considerar al delincuente informático como parte de un grupo tiene efectos en los términos de posibles negociaciones en el procedimiento acusatorio. Los preacuerdos y principios de oportunidad pueden ser aplicados a cambio de información eficaz de otros miembros de la organización, permitiéndole al fiscal conocer la ubicación y los métodos de ataque de otros miembros de la banda.

La correlación de datos y construcción de patrones. El cruce de datos no estructurados es una prioridad en las investigaciones penales modernas. La gran cantidad de información y el volumen de denuncias que llegan a diario al sistema penal acusatorio hacen imposible que se continúe con el modelo de investigación caso a caso. Para ello es necesario correlacionar y asociar cuantas investigaciones sea posible.

Hay que considerar que hay gran cantidad de información cruda que llega en la denuncia en la narración de hechos que hace la víctima, los datos contenidos en la evidencia digital recolectada y la evidencia cualitativa como testimonios, fuentes no formales, entre otros. Este tipo de datos pueden ser cruzados de forma tal que se hallen patrones de conducta particular sobre grupos o relaciones entre ataques que se desconocían. Así mismo, otras técnicas antes no usadas para el análisis de datos como la estadística y la probabilidad son de mucha ayuda en la construcción de categorías subjetivas en la imputación penal.

En mayo de 2018 se recibió por parte de una entidad financiera una denuncia en la cual ponía en conocimiento de la FGN los resultados de una auditoría interna que de forma aleatoria revisó el proceso de reintegro de dineros por fallas de ATM. Debido a que los cajeros electrónicos están expuestos a fallas que signifiquen la no entrega de efectivo, pero sí su descuento del saldo de la cuenta del cliente, las instituciones financieras en Colombia tienen diseñado un canal de quejas y reclamos que les permite conocer y solucionar el impase con la finalidad de dejar a disposición del cliente el dinero descontado lo más rápido posible.

Los resultados de la auditoría revelaron que había una concentración inusual de reclamos en un cliente específico que había recibido reintegros por fallos de cajeros de forma consecutiva en un período extendido de tiempo, razón por la cual el banco sospechaba que se trataba de un fraude. Los exámenes preliminares del perito informático verificaron que una falla en el proceso de validación del reclamo hacía que algunos terceros contratistas del banco, autorizados para acceder al sistema del ATM para recibir quejas y reclamos, permitía que se incluyesen directamente en la base de datos de reintegros, por lo que el banco entregaba abonos por este concepto casi a diario.

Aunque a partir de este punto el caso estaba bastante claro probatoriamente, el perito a cargo propuso la evaluación del sistema a partir de una prueba denominada análisis de fallos, técnica aplicada en el sector industrial para verificar la vida útil de una máquina y el promedio de fallos que presenta en su funcionamiento. Fue así como después de aplicado este análisis en la red de cajeros afectada se pudo comprobar que la probabilidad de fallos de un cajero respecto a un cliente era cercana al 1% anual y promedio de fallos por usuario era de 1,2. Comparados los resultados con los del fraude, la probabilidad de que un ATM fallase de esa forma en la realidad era del 0,0000000001%.

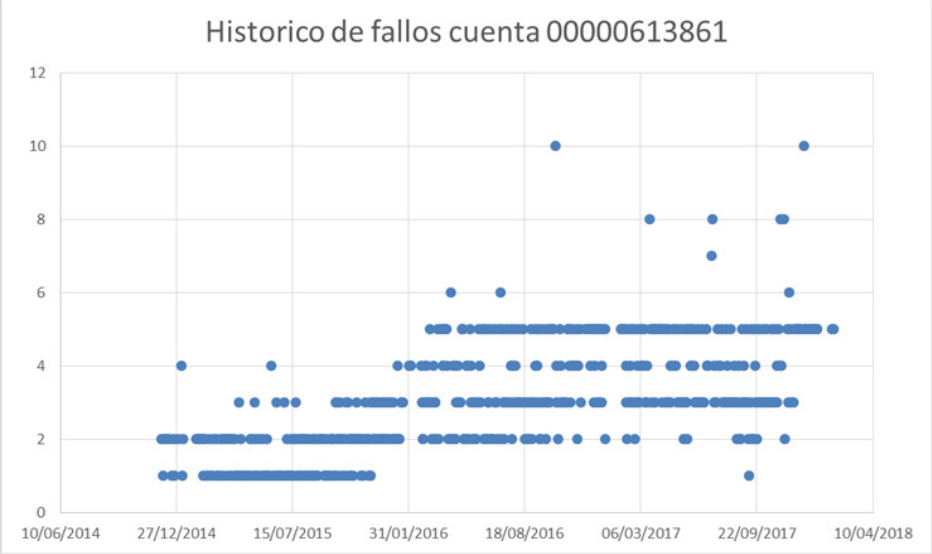


Figura 2. Distribución de fallos en la cuenta usada para el fraude de ATM. Se ve una concentración de fallos diarios que relacionan a un solo cliente, patrón que solo se presentó en este único producto financiero de todos los analizados.

Las conclusiones del análisis fueron contundentes en señalar que producto de la casualidad no podrían darse tantos fallos, por lo que se descartaba de entrada una defensa usual en juicio en este tipo de casos, la poca fiabilidad del sistema. Exhibido este análisis en la fase preliminar del proceso, los indagados aceptaron cargos en la imputación, lo que permitió una rápida evacuación del proceso del sistema judicial y una condena ajustada a los intereses de las partes.

La correlación de datos también es muy efectiva en la investigación de patrones criminales de un grupo. En el caso de los money mules o personas encargadas de prestar sus cuentas para recibir transferencias de activos fraudulentos, es común que sean personas sin mayor actividad y con poco movimiento de sus productos financieros. Aunque son las más expuestas a ser identificadas por usar datos reales en la apertura del producto bancario, acostumbran a declarar que nunca conocieron el origen de los dineros y las sumas suelen ser irrisorias, lo que descarta la posibilidad de imputar delitos con punibilidad elevada o agravantes.

Sin embargo, un cruce de estas personas en el sistema de casos de la FGN arrojó que estaban presentes en más de diez indagaciones penales por los mismos hechos, en las que solo variaba el banco y el número de producto utilizado para la transferencia de activos. El descubrimiento de este patrón habilitó al fiscal a consolidar la tesis de la existencia de una organización criminal orientada al fraude, estructurada para tal fin con la participación de los sujetos encontrados y con vocación de permanencia debido a que se pudo construir una línea de tiempo más extensa con unidad de hechos.

Este tipo de cruces puede ser igual de útil en otros tipos de investigaciones como la identificación de IP relacionadas con fraudes, horas particulares de afectación del cliente o la perfilación de la víctima por el saldo de sus cuentas o los límites transaccionales de sus productos financieros. Para que esto siga avanzando será necesario no solo compartir datos dispersos en diferentes fuentes, también es imperativo diseñar la forma como se almacenarán y procesarán con el fin de obtener información verdaderamente útil para la FGN y el sector bancario.

De la investigación reactiva a la investigación prospectiva. Uno de los retos más importantes a los que se enfrenta la administración de justicia en la lucha contra el cibercrimen tiene que ver con la necesidad de cambiar el paradigma actual de investigación penal. A diferencia de otros delitos, a pesar de poner en práctica exactamente lo dictado por manuales forenses y normativa internacional, hay aún una gran probabilidad de archivo de las investigaciones por ausencia de información que permita vincular al autor del evento.

Esto se debe a muchos factores, dentro de los cuales está la facilidad de aplicar dentro del ataque técnicas de anonimato, el uso de servidores o servicios en el extranjero, la separación física del atacante con sus víctimas o los límites normales del capital humano y técnico a disposición del fiscal en un momento determinado. Ello, sumado al gran universo de denuncias por los mismos hechos que saturan despachos a lo largo del país, hace pensar en nuevas formas de abordar el problema de la cibercriminalidad.

Una de esas soluciones está relacionada con la implementación de investigaciones prospectivas y no reactivas, implicando que el investigador judicial no llegue a los hechos después de sucedidos sino antes, previendo cuáles son los escenarios propicios que pueden ser aprovechados por el delincuente informático y adelantarse para lograr mejores resultados. Aplicada al delito informático, esto puede resultar particularmente efectivo debido a la especialización de mercados criminales explicados anteriormente.

Para ello es necesario que el investigador participe activamente de los foros de hackers donde se discute lo último en técnicas de ataque informático, se comparten nuevas piezas de *malware* y se discuten las

vulnerabilidades de los sistemas bancarios. Debido a que son abiertos y gratuitos, la información allí contenida está a la disposición de las autoridades para ser usada de la misma manera como lo hacen los criminales. Así mismo, se puede planear el rastreo de sitios físicos o virtuales donde se vendan plásticos de tarjetas, bases de datos, hardware especializado o software ilegal. Estos mercados suelen ser exitosos debido a que nadie los explora directamente dado que la atención de las autoridades se enfoca en los resultados de la acción, no en los pasos intermedios desarrollados para su ejecución. Este enfoque resulta bastante particular debido a que es una mezcla de investigación penal con labores de vigilancia y seguridad, labor que no desempeña oficialmente la FGN.

No obstante, otras instituciones, como la Policía Nacional, que desde el punto de vista constitucional desarrollan ambas funciones, han venido implementando con éxito políticas que mezclan labores de vigilancia y prevención, atención a incidentes y apoyo a la investigación penal. Un ejemplo de ello es el centro cibernético policial, que actualmente tiene a su cargo no solo la investigación del delito informático en la Dijín, sino también su prevención a través de campañas y la mejora de los canales de respuesta como el aplicativo a denunciar, desarrollado en conjunto con la FGN. Este enfoque no solo resulta más integral, sino que además disminuye los costos de transacción a la víctima, removiendo trabas que en otros casos la disuadirían de recurrir a las autoridades para denunciar.

Planeación y recolección de evidencia digital. La recolección de evidencia digital en las investigaciones por delitos informáticos es la tarea probatoria más compleja que enfrentan los equipos forenses y fiscales durante el trámite del proceso. Su dificultad radica en la volatilidad de los datos, que están siempre en riesgo de perderse o modificarse, ya sea por la misma persona que atacó el sistema, por la manipulación involuntaria de equipos afectados o por el funcionamiento normal del mismo, que le impide almacenar indefinidamente y en la forma indicada datos de interés.

Aunque no podría en ninguna circunstancia afirmar que la evidencia digital es la única información relevante en el caso teniendo en cuenta que hay un sinnúmero de evidencia documental y testimonial que también debe recolectarse, hay que considerar que esta es la encargada de probar directamente la realización del hecho en el sistema. Su análisis establecerá las circunstancias de tiempo, modo y lugar del delito informático y no puede ser reemplazada por otro tipo de elemento adicional. Por esta razón, las probabilidades de éxito del caso dependerán en gran medida de los actos urgentes que se desarrollen en las primeras horas del ataque, previendo qué datos serán útiles para probar la teoría del caso en juicio y disponer su correcta disposición como evidencia.

Este trabajo ha probado ser más difícil de lo que parece. La identificación y obtención de evidencia digital implica conocer la arquitectura del sistema afectado, los datos que prueban el hecho y descartar los que no ayudan a tal fin. También habrá que procesarlos de manera que puedan demostrar al juez y las partes de forma clara y precisa las circunstancias acaecidas. Con ello se puso de presente la necesidad de desarrollar una metodología orientada a ayudar a fiscales e investigadores a planear toda la fase de investigación pensando en la eficiencia como principio básico de grupos con escasez de recursos humanos y técnicos.

Como punto de partida, el fiscal y sus investigadores deben considerar la taxonomía del ataque informático, una técnica ampliamente usada en la ciberseguridad y que se enfoca en la detección de amenazas y vulnerabilidades sobre un sistema informático con el fin de corregirlas y preparar planes de contingencia en caso de fallos. Además de ser muy útil por ser la misma metodología que están aplicando los equipos de respuesta cibernética, lo que de entrada deja conceptualmente en los mismos términos a estos con los equipos forenses, resulta muy eficaz para determinar elementos que luego tendrán relevancia penal.

En una taxonomía básica es necesario determinar datos como el atacante, la herramienta informática usada y la vulnerabilidad que explota, la identificación del sistema afectado y la acción concreta que se ejecutó sobre este; determinando específicamente qué resultados tuvo sobre los datos, componentes lógicos o físicos que lo integran. En esta primera identificación es importante resaltar que los equipos de respuesta a incidentes ya están trabajando en la reconstrucción de estos hechos, por lo que el trabajo de respuesta y el de investigación tienen en la primera fase los mismos objetivos.

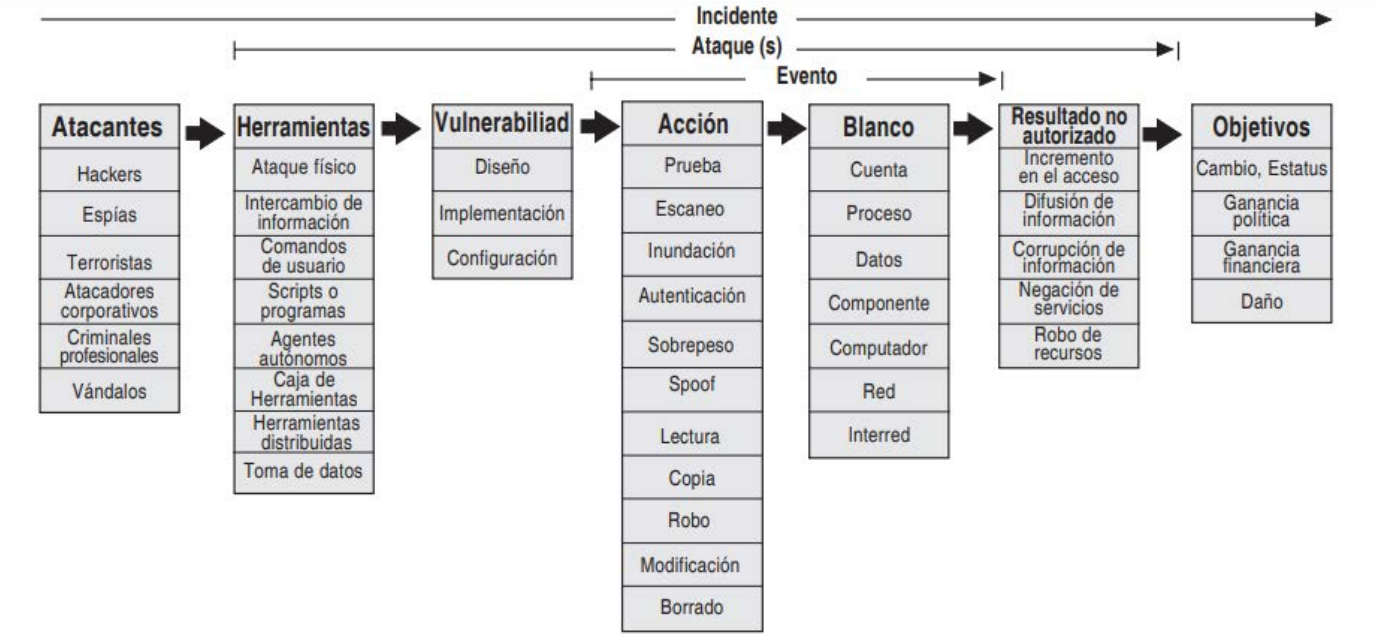


Figura 3. Modelo teórico de una taxonomía de ataque, identificado las variables más importantes del incidente y su relación con los efectos en el sistema afectado.

Esta sucesión de eventos debe ser organizada de forma gráfica, ubicándolos de tal manera que se puedan apreciar los sistemas informáticos involucrados, los datos afectados o recolectados en el ataque y las amenazas aprovechadas por el autor del delito. Esta representación de los hechos no solo le hace más fácil al fiscal identificar dónde se podría encontrar la evidencia digital, también puede ser de ayuda como evidencia demostrativa en las audiencias subsiguientes donde se tendrá que explicar lo sucedido al juez y demás partes e intervinientes, menos conocedores de los aspectos técnicos del caso.

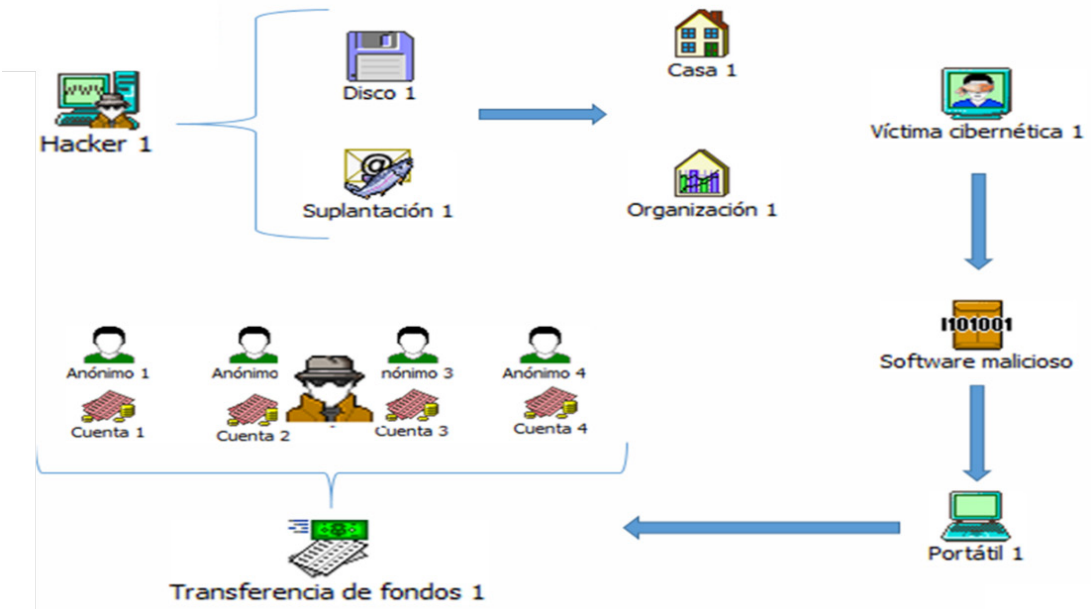


Figura 4. Modelo de taxonomía de ataque simplificado para una investigación real. La gráfica muestra el sujeto activo, el medio de infección y la herramienta usada, los sistemas afectados y los beneficiarios de las transacciones ilegales. Este modelo simplificó en audiencia la presentación del caso.

Identificados los hechos, hay que hacer dos consideraciones jurídicas importantes. La primera tiene que ver con la evidencia digital disponible con la finalidad de determinar cuál de estas requiere algún tipo de autorización judicial y cuál no. Si la información se refiere a datos que relacionan directamente al indiciado o contienen datos personales sensibles de este o de terceros, habrá que considerar que el perito no puede iniciar su recolección hasta que un juez de control de garantías evalúe los motivos fundados que rodean la orden y permita el acceso a los mismos. También habrá que ponderar qué datos informáticos son los más volátiles y enfocar la labor de recolección y autorización judicial a estos, dado que son los que tienen más posibilidad de perderse con el pasar del tiempo.

Igualmente habrá que considerar también cuales fueron los resultados dentro del sistema con el fin de conocer qué tipo de delito se pudo haber cometido. No todas las técnicas tienen el mismo fin: algunas, como el ataque DDOS, están orientadas a la inhabilitación de un sistema y otras, como los ataques de fuerza bruta, están diseñadas para lograr accesos abusivos. Dado que los ataques informáticos tienen infinidad de clasificaciones técnicas que pocas veces tienen identidad con las categorías jurídicas del título VII Bis del Código Penal, es más útil considerar los daños o acciones dentro del sistema para descubrir el posible delito aplicable.

De esta forma, un ataque informático se basará, en la mayoría de los casos, en:

Técnicas de acceso ilegal: orientadas a lograr el acceso de un tercero al interior de un sistema informático. Estas no incluyen necesariamente alguna acción adicional ya que se centran en lograr exclusivamente el ingreso al sistema afectado. Ejemplos de ello son los ataques de diccionario para descifrar claves de acceso o la suplantación de identidad (spoofing) de sitios web para la captura de los datos de validación de la víctima.

Técnicas contra la confidencialidad: están diseñadas para la captura de datos confidenciales, estén estos en tráfico, como el caso de las interceptaciones ilegales, o en bases de datos, como la obtención y uso de datos o códigos personales. Tecnologías de transmisión inalámbica son especialmente vulnerables a este tipo de ataques.

Técnicas contra la disponibilidad del sistema: están orientadas al sabotaje de un sistema informático, evitando que desempeñe las funciones para las cuales fue programado o las ejecute de forma diferente. Se enmarcan en esta categoría los ataques de denegación de servicio o el buffer overflow. Técnicas contra la integridad: son ataques que modifican o alteran las propiedades de cualquier elemento de un sistema. En este caso esa modificación no pone en riesgo el funcionamiento de este, pero altera la estructura o programación del sistema. Un ejemplo de esta técnica es el ransomware o cualquier otro *malware* que afecte la integridad de los datos alojados en un disco.

Debido a que la Ley 1273 de 2009 consagró el bien jurídico tutelado de la información y los datos y consagra textualmente los "atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y los sistemas informáticos", cualquiera de las técnicas antes clasificadas se ajustará a alguno de los delitos allí descritos, lo que le facilita al fiscal determinar con claridad el conjunto de tipologías penales que investiga.

La aplicación de este modelo de investigación no solo mejora la planeación de la investigación de delitos informáticos, también ayuda a distribuir de mejor manera las tareas de investigación forense en los laboratorios. En la FGN actualmente los grupos de informática forense no solo se dedican a la investigación de delitos informáticos, también asesoran en la recolección de la evidencia digital de otras investigaciones que lo requieran. La extracción de información de computadores personales, celulares, circuitos cerrados de televisión o sistemas contables son muy comunes, saturando el personal técnico en labores sencillas como la conservación de documentos digitales. Esto ha dejado menos tiempo para investigaciones con mayor complejidad como el análisis de *malware* o de logs de sistemas informáticos.

Mejorar las cargas de trabajo de los laboratorios implica la desconcentración de las actividades de conservación, que son menos complejas, en investigadores capacitados para ello, dejando las tareas de análisis a peritos con más experiencia. A manera de un triage, estas investigaciones pueden ser clasificadas de acuerdo con su urgencia y complejidad, verificando que cada una de ellas esté asignada al funcionario más capacitado. Así mismo, es importante no dejar de avanzar con las técnicas de análisis. Conservar el elemento material probatorio es un paso muy importante pero insuficiente; ello solo deja un compilado de datos sin analizar que deben ser valorados para establecer su utilidad dentro del proceso.

Es muy común encontrar casos en los que se recolectaron cientos de discos de información sin mayores resultados debido a que las horas-hombre necesarias para analizarlas superaban por mucho la capacidad de los investigadores asignados. Esto suele matizarse progresivamente con la introducción de softwares de correlación automática de patrones y otras herramientas de IA, por lo que quedará de nuevo en manos de fiscales y jueces su uso y compresión en casos futuros.

Conclusiones

La investigación de delitos informáticos es uno de los retos más importantes que enfrentan jueces y fiscales actualmente. Su complejidad técnica, el deber de celeridad que impone la recolección de evidencia digital, así como las condiciones especiales de este fenómeno criminal imponen cargas nuevas a los investigadores y equipos jurídicos de la FGN. Algunos de estos cambios resultan ser realmente radicales, como la virtualización de la escena del crimen, la inexistencia de barreras geográficas y la concurrencia de jurisdicciones en los casos más simples.

La búsqueda de soluciones a este tipo de problemas impone a las partes involucradas, ya sean víctimas, agencias de investigación u operadores de TI, encontrar de manera conjunta estrategias de mitigación del delito y mejora de los procesos de colaboración en el marco de la investigación penal. El crecimiento del cibercrimen en Colombia y en el mundo en general se debe a externalidades que no han sido apropiadamente valoradas. La facilidad de conseguir las herramientas de hackeo, el anonimato, la existencia de países con regulaciones informáticas laxas y la cooperatividad han hecho que cualquiera con suficiente motivación ingrese al mercado del delito informático sin mayores costos de transacción.

Muy al contrario, las partes afectadas se mantienen en estructuras rígidas y poco colaborativas que no solo hacen difícil la investigación de un caso, sino también facilitan las circunstancias que motivan al delincuente. Una formulación de una política criminal efectiva en estos casos debe tener como prioridad la generación de incentivos de mercado a todas las partes de forma que se comporten racionalmente como sus contrapartes criminales. Ello implica el valorar los costos verdaderos del problema, especialmente a largo plazo y retirar barreras para trabajar de forma cooperativa.

Las reformas legales son insuficientes en este aspecto. Hasta ahora se han enfocado en agudizar penas bajo la creencia extendida de que el punitivismo por sí solo es suficiente para disuadir los comportamientos criminales. Además de ser soluciones a largo plazo por la complejidad de impulsar este tipo de proyectos, suelen ser ineficaces si no se incluyen medidas que aumenten la probabilidad de éxito en las investigaciones. Por ello es importante partir con políticas que optimicen los recursos existentes y mejoren los procesos aplicados en ellos.

La mejora de los procedimientos de identificación, recolección, análisis y presentación de la evidencia garantizará el material necesario para enjuiciar a los autores materiales y el trabajo conjunto permitirá la correcta coordinación de esfuerzos de todos los involucrados, lo que a mediano plazo bajará el costo marginal de atender cada denuncia presentada y disminuirá el número de entradas al sistema penal, dejando más tiempo a fiscales e investigadores para centrarse con profundidad en los casos restantes.

Referencias

Becker, G. S. (Marzo-abril 1968). Crime and Punishment: An Economic Approach. The Journal of Political Economy, 76(2), 169-217.

Broadhurst, R. (s.f.). Developments in the global law enforcement of cyber-crime. (Q. U. Technology, Ed.) Policing: An International Journal of Police Strategies and Management, 408 - 433.

Broadhurst, R., Grabosky , P., Alazab, M., & Chon, S. (Enero/junio 2014). Organizations and Cybercrime: An analysis of the nature of groups engaged in cybercrime. International Journal of Cyber Criminology, 8(1), 1-20.

Brown, C. D. (Junio 2015). Investigating and Prosecuting Cybercrime: Forensic dependencies and Barriers to justice. International Journal of Cyber Criminology, 9(1), 55-119. doi:10.5281/zenodo.22387

Ciarduaín, S. Ó. (2004). An Extended Model of Cybercrime Investigations. International Journal of Digital Evidence, 3(1).

Foester, L. (2016). Cybercrime as a global issue: Finding solutions through interdisciplinarity and strengthened cooperation. Obtenido de https://www.researchgate.net/publication/302908128

Kshetri, N. (Enero-febrero 2006). The Simple Economics of Cybercrimes. IEEE Security and Privacy, 4(1), 33-39.

Kshetri, N. (2009). Positive Externality, Increasing Returns and the Rise in Cybercrimes. Communications of the ACM, 52(23), 141-144. doi:http://doi.acm.org/10.1145/nnnnnn.nnnnnn

Moore, T., Clayton , R., & Anderson , R. (2009). The Economics of Online Crime. Journal of Economic Perspectives, 23(3), 3-20.

Wori, O. (2014). Computer Crimes: Factors of cybercriminal activities. International Journal of Advanced Science and Information Technology, 3(1), 51-67.

Capacidades jurídicas y de informática forense en Colombia: desafíos en ciberseguridad

Santiago Castiblanco Hernández, María Camila Barrera, Andrés Quijano, Jaime Rincón

Introducción

El sector financiero es un componente esencial en el desarrollo de la economía de los países. Un sistema financiero sano permite la inversión de capital en actividades productivas, expande los mercados, recauda ahorro, transfiere riesgos e interviene en el proceso de formación de precios. Además, en los últimos años con la disrupción tecnológica, el sector financiero ha elevado su nivel de productividad y capacidad de prestación de servicios a los usuarios. De igual manera, en los últimos años el internet y el desarrollo de tecnologías de la información han permitido que la sociedad se encuentre cada vez más conectada, trayendo consigo un mayor dinamismo, innovación y oportunidades de crecimiento económico.

Sin embargo, a la par de estos avances tecnológicos, se ha incrementado el número de ataques cibernéticos, siendo el sistema financiero uno de los principales blancos de ataque y de materialización de fraude a través de técnicas informáticas. De acuerdo con estudios del Fondo Monetario Internacional, el promedio de las posibles pérdidas anuales resultantes de los ataques cibernéticos puede ser significativo y ubicarse en el orden del 9% de los ingresos netos de los bancos a nivel mundial (Fondo Monetario Internacional, 2018).

El nivel de penetración de estas tecnologías en el sistema financiero colombiano se observa en la tendencia al alza en el uso de canales no presenciales. Al cierre de 2018, el 56,01% del monto total de las operaciones se realizaron a través de estos canales (internet, telefonía móvil, débito automático, ACH e IVR), lo que se traduce en un poco más de $4.023 billones (Superintendencia Financiera de Colombia, 2019). Asimismo, los ataques cibernéticos y las modalidades de fraude cibernético contra el sistema financiero y servicios de pago del país han venido evolucionando, al punto que actualmente resultan relevantes modalidades como fugas de información, *phishing*, uso de *malware, carding,* suplantación de clientes, *ransomware*, así como de actividades delictivas de ingeniería social para la materialización de fraude.

El mayor uso de canales digitales y no presenciales ha generado mayor interconectividad, facilidad de uso y reducción de costos, pero también mayores riesgos de fraude, siendo así el sistema financiero uno de los más afectados debido a delitos informáticos en Colombia. De acuerdo con cifras de Asobancaria, para el 2018 el fraude en ambiente no presente en el sistema financiero de Colombia representó el 58,5% del fraude total (2019), concentrándose principalmente en la categoría de tarjetas de crédito y cuentas de ahorro y corriente.

Teniendo en cuenta lo anterior, el presente documento pretende aportar evidencia de la evolución de las capacidades y retos que afronta el sistema judicial en Colombia frente a esta tipología de delitos. En particular se busca mostrar el impacto de capacitaciones y cursos especializados en las capacidades de investigación judicial en delitos informáticos de la Fiscalía General de la Nación. Asimismo, se expondrá cómo algunos miembros de la industria bancaria nacional han desarrollado estrategias para enfrentar estas

amenazas en los últimos años y su efecto sobre sobre la gestión del riesgo cibernético en sus entidades. Para ello, en primer lugar, se situarán las capacidades institucionales, legislativas y de política pública con las que cuenta Colombia en la gestión del riesgo de ataques cibernéticos. Seguido de ello, se presentarán los resultados de entrevistas a fiscales de la Fiscalía General de la Nación que manejan este tipo de casos, buscando evidenciar los retos actuales y las principales herramientas con las que cuentan para judicializar. En tercer lugar, se mostrarán los principales resultados de entrevistas a jefes y directores de seguridad de algunas entidades bancarias frente a los ciberdelitos, y finalmente, se presentará una serie de recomendaciones de estrategia y política para la disminución y gestión del riesgo cibernético, a su vez algunas iniciativas que han surgido desde el sector privado que se espera que ayuden a reducir el impacto y alcance de este tipo de delitos.

Avances en política pública, diseño institucional y normativo e iniciativas desde el sector privado

Tradicionalmente se asocia el primer acercamiento institucional a temas de tecnología y comercio electrónico desde el punto de vista jurídico a la Ley 527 de 1999, tratando temas como la validez jurídica de mensajes de datos y los atributos de la firma digital. En 20 años, la creación de mecanismos, instituciones y de políticas públicas evidencian como el país ha desarrollado un marco normativo que lo ha posicionado como el sexto país del continente en el índice mundial de ciberseguridad (International Telecommunication Unit, 2017). Como respuesta a los nuevos desafíos en ciberseguridad que enfrenta el sistema financiero y las implicaciones que tiene, dada la alta interdependencia con otros sectores, han surgido diversas iniciativas de política pública, institucionales y legislativas, que se han complementado con estrategias gremiales dirigidas a prevenir y mitigar los riesgos de fraude y ataques cibernéticos en el país.

Dentro de los diferentes avances normativos y política pública de estos 20 años en temas de ciberseguridad, caben destacar la Ley 1273 de 2009, el Documento CONPES 3701 de 2011 y el Documento CONPES 3854 de 2016, los cuales serán expuestos a continuación.

La Ley 1273 de 2009 modifica el Código Penal para crear "un nuevo bien jurídico tutelado – denominado 'de la protección de la información y de los datos' y preserva integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones". De esta manera, se adicionan al Código Penal delitos informáticos que atentan contra la seguridad de los ciudadanos y del país, brindando un marco punitivo para este tipo de crímenes e inicios para su correcta judicialización, buscando modernizar la regulación penal para quedar a tono con lo suscrito en el Convenio sobre Cibercriminalidad en Budapest[144] en 2001 (Remolina, 2010).

El Documento CONPES 3701 estableció los lineamientos de política de ciberseguridad y defensa con el objetivo de fortalecer las capacidades del Estado, fortaleciendo la institucionalidad y legislación del país en este aspecto, a la vez que señala la necesidad de brindar capacitación especializada en seguridad de la información a funcionarios que estén involucrados con estos temas como fiscales y jueces. A partir de este Documento se da pie a la implementación de organismos especializados como el Grupo de respuesta a emergencias cibernéticas de Colombia ColCERT, el Comando Conjunto Cibernético (CCOC) de las FF. MM. y el Centro Cibernético Policial (CCP), entre los cuales se coordinan asistencia técnica y se da colaboración activa en la resolución de incidentes.

El Documento CONPES 3854, por su parte, evalúa los alcances y logros que tuvo el CONPES 3701, identificando que el principal éxito fue el desarrollo de instituciones que permiten hacerle frente a estos crímenes, a la vez que plantea que el enfoque necesario es involucrar a las múltiples partes interesadas, quienes desarrollan parte o todas sus actividades socioeconómicas en el entorno digital, promoviendo condiciones para que estas gestionen y mitiguen los diversos riesgos cibernéticos en sus actividades. Cabe mencionar que este CONPES trata el tema de ciberseguridad no solo desde una esfera de seguridad y defensa nacional sino con el fin de contribuir al desarrollo de la economía digital del país, preservar los derechos humanos y valores fundamentales de las personas, protegiéndolos frente a las amenazas.

La participación de los diversos grupos sectoriales que realizan parte de sus actividades a través de tecnologías en temas de ciberdefensa se evidencia en la membresía de nueve CSIRT[145] en el Foro de equipos de seguridad y respuesta de incidentes –FIRST- (Forum of Incident Response and Security Teams, 2019). En particular para el sector financiero se cuenta con un Grupo de Respuestas a Emergencias Cibernéticas – CSIRT financiero y un plan de defensa sectorial.

Sumado al desarrollo de política pública e institucional, Colombia cuenta con avances legales y normativos, entre los que se encuentran la Ley 1266 de 2008 y 1581 de 2012 de Habeas Data, la Circular Externa 007 de 2018 de la Superintendencia Financiera la cual imparte instrucciones relacionadas con los requerimientos mínimos para la gestión del riesgo de ciberseguridad y la Resolución 3067 de la Comisión de Regulación de Comunicaciones de 2011 la cual establece que los proveedores a acceso a internet deben utilizar los recursos técnicos y logísticos tendientes a garantizar la seguridad de la red. Tomando esto en cuenta, resulta relevante la promoción del desarrollo y fortalecimiento de capacidades sectoriales para proteger al usuario y al mismo tiempo velar por el desarrollo económico del país.

Finalmente, como fue mencionado en el CONPES 3701 en 2011, era necesaria la capacitación especializada al personal de la rama judicial, puesto que para esa época la oferta académica y de cursos sobre el tema era escasa. Actualmente se ha experimentado un crecimiento de cursos académicos y foros disponibles en temas de ciberseguridad en el que participan universidades, entidades privadas y organismos policiales, incluyendo maestrías y programas de acreditación (el Banco Interamericano de Desarrollo y la Organización de los Estados Americanos, 2016).

Cabe resaltar la participación de Asobancaria en la realización de este tipo de cursos, brindando patrocinio o sirviendo como facilitador de foros y paneles de autoridades en el tema.

Entrevistas a fiscales: retos y herramientas en la judicialización de ciberdelitos

Asobancaria realizó entrevistas a Diana Marcela Romero y Héctor Andrés Daza, fiscal delegada antes jueces municipales y fiscal delegado ante jueces del circuito de Bogotá, respectivamente, los cuales han manejado casos de ciberdelitos, con el propósito de exhibir opiniones del marco jurisprudencial colombiano y los retos que enfrentan actualmente miembros de la Fiscalía General de la Nación, a su vez de contar con sus percepciones de mejora para enfrentar el cibercrimen.

La fiscal Diana Romero, miembro de la Unidad de Hurtos Informáticos, considera que actualmente la jurisprudencia frente a ciberdelitos ha sido insuficiente, puesto que ha abarcado este tipo de crímenes como delitos contra el patrimonio económico dejando de lado la vulneración a datos y la seguridad de

sistemas informáticos, lo que no ha permitido una tipificación penal que abarque la totalidad del delito, dándose así el relativamente poco contenido de temas de seguridad cibernética en el derecho civil. A su vez, los jueces de la judicatura no cuentan con el conocimiento adecuado en este tipo de delitos dado lo técnico de los elementos. Esto, junto a la falta de jurisprudencia, evita que los jueces tomen decisiones que analicen el cibercrimen desde las diversas implicaciones y vulneraciones que trae consigo, sino tratando el delito como un simple hurto.

En este sentido, nos comentó que las capacitaciones que reciben los fiscales en tipología y la terminología de los ciberdelitos permiten "abrir la expectativa del delito", ya que con la capacitación se entiende cómo continuar con la investigación del caso y correlacionar casos para hacer esfuerzos en detección y estructuración de bandas delictivas que cometen estos delitos.

El fiscal Héctor Daza, el cual hace parte de la Unidad de Estructura de Apoyo, la cual maneja el fenómeno criminal de organizaciones criminales de Bogotá, argumenta de igual manera que seminarios y capacitaciones en temas relacionados con sistemas e informática han permitido que los fiscales tengan claridad en aspectos técnicos de los casos de este tipo, al tiempo que se generan vínculos investigativos y de colaboración entre la academia y la Fiscalía. Asimismo, comenta que es necesario que más fiscales y jueces participen en estos espacios. Finalmente, menciona que la Ley 1908 de 2018 es un gran avance en el marco legal para combatir el ciberdelito, si bien aún falta trabajar en su implementación.

En cuanto al comportamiento de los criminales, ambos fiscales comentan que se ha percibido cambios en el sentido que, al evolucionar las herramientas y las acciones tomadas en contra de un crimen en específico, los delincuentes pasan a otra modalidad delictiva, de la misma manera que atacan las vulnerabilidades que se pueden detectar en entidades -no precisamente financieras-. Ante esto, señalan que es necesario que, las entidades estatales en particular, al manejar grandes recursos, reciban capacitaciones de seguridad y de prevención frente a este tipo de delitos. Asimismo, comparten que la ingeniería social[146], las fugas de información de bases de datos y suplantación de SIMCard, son los principales ciber delitos que manejan actualmente.

Ambos fiscales están de acuerdo en que aún hace falta trabajar en la educación financiera de los clientes y dan como ejemplo el mal manejo de productos y las malas prácticas de los clientes, como revelar la contraseña de la tarjeta débito o el código CVV de la tarjeta crédito. De igual forma, destacan la gran importancia del uso apropiado de estos como herramienta de prevención del fraude.

El fiscal Héctor Daza, sostiene que, si bien las actuales billeteras móviles facilitan varias transacciones para los cuentahabientes, ocurren casos en los que estos no tiene conocimientos básicos de protección de la información, por lo que son susceptibles a través de estas aplicaciones a ser víctimas de fraude. Por su parte, la fiscal Diana Romero comenta que del promedio de casos que manejan por mes, uno o dos procesos son delitos cometidos por personas con un alto nivel de conocimiento de ingeniería, y que la mayoría de las denuncias se refieren a temas relacionados con robos de bases de datos.

Finalmente, la fiscal Diana Romero señala como oportunidades de mejora el conocimiento de la policía judicial de este tipo de crímenes y propone que este grupo reciba formación sobre el tema, sin descuidar las capacitaciones a los fiscales e investigadores. Asimismo, comenta que la cooperación entre bancos y Fiscalía debe ser mayor y de esta manera se pueda prevenir las amenazas.

Por su parte, el fiscal Héctor Daza considera que los avances jurisprudenciales que podrían facilitar la investigación y contribuir a enfrentar el ciberdelito deben darse en el manejo y recaudo de la evidencia cuando esta es volátil frente a su legalización. De igual manera menciona que debido al rol primordial

que han adquirido los dispositivos móviles en la vida diaria, la creación de un marco normativo en el desarrollo de aplicaciones móviles relacionadas con servicios financieros permitiría que se reduzcan los casos de fraude que se presentan en esta modalidad. Igualmente, expresa que se les debe explicar a los clientes el manejo de los servicios y productos para clientes, de manera que dependiendo de los que usan, teniendo en cuenta su familiarización con estos (generaciones más jóvenes conocen mejor y les dan mejor uso a portales no presenciales, mientras que es menor en las mayores), prevendría y evitaría el fraude que se comete por desconocimiento.

Entrevistas a directores de seguridad bancarios: percepciones de la banca ante los ciberdelitos

Por parte de Asobancaria se realizaron entrevistas a Jorge Mario Rodríguez, director de seguridad de la información del Banco Caja Social, Gabriel Lasso Ramírez, gerente de ciberseguridad y riesgos de tecnología del banco BBVA y Anuar Torres, director de riesgo transaccional del banco Davivienda. El objetivo fue exponer cómo algunos miembros de la industria bancaria nacional han desarrollado estrategias para enfrentar los delitos informáticos y amenazas cibernéticas en los últimos años.

En temas de jurisprudencia y cooperación judicial, Jorge Rodríguez opina que el marco judicial, que brinda un marco para tratar este tipo de delitos, en la mayoría de los casos está rezagada, puesto que la naturaleza del ciberdelito hace que este avance y se transforme continuamente, más rápido que las normas. De igual manera, destaca que los esfuerzos internacionales como el Convenio de Budapest son herramientas que ofrecen un buen marco para tratar con estos temas desde el aspecto legislativo.

Asimismo, Rodríguez percibe que sí hay cooperación con autoridades como la Fiscalía y la DIJIN, aunque opina que el número de fiscales y jueces que cuentan con capacitación penal para tratar este tipo de delitos es reducida, por lo tanto, el manejo de las denuncias se puede complejizar. En el mismo sentido, afirma que la capacitación dentro de las entidades bancarias tiene que ser permanente por las nuevas tecnologías y formas de actuar a las que tienen acceso y realizan los criminales.

Anuar Torres opina que hay un buen marco regulatorio que toca puntos sensibles, y reconoce que la fiscalía cada vez cuenta con recursos más especializados y con personal que entiende y comprende de delitos informáticos. Sin embargo, los procesos no fluyen a la velocidad con que se desea y los resultados se ven dilatados. De igual manera, percibe que a nivel judicial hay temas de cooperación e intercambio de información, pero que desafortunadamente los resultados no son rápidos.

Por su parte, Gabriel Lasso considera que la ley 1273 de 2009 y las diferentes leyes subsiguientes tienen puntos interesantes, pero la agilidad del proceso judicial afecta la judicialización de este tipo de casos. Por esto, es necesario buscar alternativas desde la legislación, aparato judicial y de investigación para ayudar a reducir los tiempos y mejorar el sistema actual.

En temas de cooperación, Lasso comenta que nunca es suficiente, siendo necesario cooperar y compartir información contra el cibercrimen. Si bien hay cierto nivel de recelo tanto en entidades estatales como privadas, en los casos en que se ha compartido información, se han visto resultados importantes, mencionando así el comité de ciberseguridad y prevención del fraude que realiza la Asociación Bancaria. Este ha sido un espacio en el que se comparte información como tendencias y técnicas que se han detectado, abriendo espacios de colaboración entre el Estado, banca y entes reguladores buscando mejorar y reducir las posibilidades de fraude. Teniendo en cuenta esto, indica que se debe seguir desarrollando marcos de colaboración.

En cuanto a prevención del fraude en las entidades financieras, Torres señala que en la entidad entienden el fraude como un fenómeno transversal a la organización que afecta a los clientes y a todos los actores que intervienen en el proceso. Por lo anterior, cuentan con una estructura de gobierno especializada para la gestión de riesgo de la ciberseguridad, siendo un comité ejecutivo de alto nivel el que se encarga de esta problemática. Este comité se encuentra articulado con áreas especializadas en la analítica para la gestión de los riesgos de ciberseguridad y fraude, analítica transaccional, gestión de alertas y monitoreo en medios de pago, y la configuración de la funcionalidad de la transaccionalidad de los canales, integrándose esto bajo un solo proceso y ejecutándose de manera especializada por las diferentes áreas de la organización.

Rodríguez comenta que las estrategias para prevenir el fraude en su entidad están orientadas a mejorar la seguridad de la información, garantizar la ciberseguridad dentro del ciclo de vida de los productos financieros que ofrecen, concientizar al usuario, asegurar la protección de la información (clasificación de información crítica), gestionar los riesgos y fortalecer el monitoreo de los activos. De igual manera, dentro de la cultura organizacional del banco se han creado estándares para contratar terceros, los cuales son seguidos por todas las áreas. A su vez, se ha logrado la concientización de prácticas seguras con la información que manejan.

Por su lado, Lasso menciona que una buena práctica en su entidad es la detección de transacciones fraudulentas; de la mano del monitoreo transaccional se encuentra el acompañamiento de manera segura al usuario de la banca digital -disponiendo de canales transaccionales adecuados y sencillos-, lo que facilita que los clientes adopten estrategias seguras y conscientes de su seguridad.

Tanto Lasso como Rodríguez sostienen que actualmente los cibercrímenes contra la banca colombiana no son perpetrados utilizando técnicas avanzadas de ataque y que se utilizan herramientas que no requieren un alto conocimiento en sistemas o preparación técnica. Si bien Rodríguez señala que en Colombia hay un grado de conocimiento importante, por ahora no considera que la mayoría de los ataques perpetuados sean realizados por criminales con un alto grado de preparación, como ha ocurrido en Chile o México, donde es posible que existan hackers patrocinados por estados. A su vez, Lasso expresa que la mayoría de los ataques ocurren por la facilidad de cometer este tipo de delitos (se pueden adquirir servicios criminales como *malware*, ataques, entre otros) pero no necesariamente son perpetuados por personas con gran expertise.

Por su parte, Torres encuentra que cada vez hay organizaciones criminales más estructuradas, con distintas capas, cada una con un cierto nivel de especialización o conocimiento específico, por lo que los conocimientos técnicos varían según el nivel en el que se encuentre el delincuente en la organización (planeación del primer ataque, conocimiento del funcionamiento de los sistemas y canales transaccionales de cada banco, materialización del delito, etc.) Adicionalmente encuentra que estas organizaciones tienden a ser transnacionales.

De igual manera, todos los entrevistados concuerdan con que la educación financiera juega un rol primordial en prevención del ciberfraude. Rodríguez opina que cuánto más se piense en los usuarios como ciberciudadanos, más fácil será la enseñanza y la concientización en el uso de nuevas tecnologías y servicios financieros, y permitirá la reducción del nivel de exposición de las personas a los ataques cibernéticos. A su vez, Lasso manifiesta que debido a que la ingeniería social busca engañar al cliente para que este entregue su información confidencial bancaria, la educación y formación financiera para evitar que el cliente no caiga en este tipo de engaños son actividades que deben fortalecerse, al tiempo que la formación y estrategia de comunicación a cada sector de la población debe ser focalizada teniendo en cuenta sus características. Torres presenta que más allá de la educación financiera debe haber cultura de

prevención del fraude, lo cual involucra no solo a los clientes sino a todos los integrantes del ecosistema financiero.

Por último, al pedirles a los entrevistados sugerencias para atacar el ciberdelito, se encontraron los siguientes comentarios:

Torres expone que las denuncias son analizadas por diferentes entidades que realizan investigaciones, pero que estas no se articulan entre sí. Se hace necesario que existan órganos conjuntos entre autoridades, industria y clientes que puedan coordinar una gestión permanente del delito, ya que actualmente las instituciones trabajan por casos, sin compartir información. Esto, junto a la complejidad del sistema judicial, da como resultado que la obtención de resultados sea difícil. En vista de esto, articular entre todos los actores un proceso de investigación continuada y permanente resulta se considera una gran oportunidad.

Lasso opina que el aparato judicial y de investigación del Estado debe contar con mayor colaboración y prontitud entre entidades, comercios y el Estado, para permitir cerrar brechas que pueden detectar los ciberdelincuentes para afectar a los ciudadanos.

Rodríguez arguye que es necesario fortalecer equipos de respuesta a incidentes, de tal manera que actúen rápidamente, con un énfasis preventivo y que cuenten con tecnología y capacitaciones para la realización de sus tareas; compartir información para hacer seguimiento a amenazas comunes de cualquier sector; mayor rapidez en la judicialización de estos casos y contar con fiscales e investigadores que se encuentren especializados en este tipo de delitos. Finalmente considera importante la realización de foros continuos que involucren el poder judicial y el desarrollo de temas que abarquen la informática forense por parte de las universidades.

Conclusiones y observaciones para enfrentar el ciberdelito en Colombia

Si bien el objetivo del presente estudio es mostrar y señalar las oportunidades y retos del sistema judicial para enfrentar el ciberdelito en el país, se considera pertinente mencionar algunas de las iniciativas que desde el sector privado se han llevado a cabo, gracias al impacto que han tenido en los indicadores de fraude. Estas iniciativas no necesariamente son alejadas de la agenda de prevención del ciberfraude diseñada por el gobierno y entidades gubernamentales.

Entre las medidas originadas desde el sector privado se destaca la incorporación de un microchip a las tarjetas bancarias tanto de débito como de crédito. Esta tecnología -que comenzó a ser implementada a principios del 2000, desarrollada por Europay, MasterCard y Visa- protege los datos del tarjetahabiente, que estaban expuestos a ser vulnerados mediante la técnica de *skimming*. Eventualmente, este avance tecnológico adquirió relevancia en la agenda de política pública del país, evidenciada en la Circular Externa 052 de 2007, que da instrucciones relacionadas con los requerimientos mínimos de seguridad y calidad en el manejo de información a través de medios y canales de distribución de productos y servicios para clientes y usuarios" (Superintendencia Financiera de Colombia, 2007). Igualmente, la Circular Externa 042 de 2012 "por medio de la cual se incorporan algunas modificaciones (...) en materia de requerimientos mínimos de seguridad y calidad para la realización de operaciones" (Superintendencia Financiera de Colombia, 2012) establece mecanismos internos de autenticación fuerte que son utilizados actualmente.

Por otro lado, recientemente en Asobancaria se han desarrollado mesas de trabajo entre franquicias de tarjetas bancarias, redes procesadoras de pago, pasarelas de pago y entidades bancarias para desarrollar una instauración integra de medidas como tokenización y protocolos de seguridad como 3DSecure o basados en este. A su vez, la Superintendencia Financiera, mediante la Circular Externa 007 de 2018 "imparte instrucciones relacionadas con los requerimientos mínimos para la gestión del riesgo de ciberseguridad" (Superintendencia Financiera de Colombia, 2018) y la Circular Externa 008 de 2018 "imparte instrucciones en materia de requerimientos mínimos de seguridad y calidad para la realización de operaciones" que involucran a las pasarelas de pago (Superintendencia Financiera de Colombia, 2018). Se demuestra otra vez la importancia que tienen las medidas de seguridad eficientes en los diversos canales con los que cuenta la banca actualmente. Teniendo en cuenta lo anterior y la experiencia con la inclusión de microchip en años pasados, la innovación en temas de seguridad en la banca puede influir en las políticas que desarrollan las entidades estatales hacia este sector, por lo que la cooperación entre ambas partes juega un papel fundamental en su buen desarrollo y ejecución.

De igual manera, Asobancaria ha elaborado un convenio con la Fiscalía General de la Nación para reducir los tiempos en el intercambio de información en investigaciones a clientes relacionados con temas de ciberseguridad y fraude. Actualmente la entrega de documentos y folios se realiza de manera física -lo que trae consigo demoras y posibilidades de pérdida de la información– mientras que el convenio contempla el envío de información mediante plataformas digitales. Este tipo de iniciativas agilizarían los tiempos de judicialización, aspecto que es señalado como oportunidad de mejora por algunos de los entrevistados.

A partir de las entrevistas a fiscales que tratan los ciberdelitos y directores de seguridad de algunas de las entidades financieras del país, se encuentran puntos en común. Cabe resaltar que las entrevistas son usadas como un instrumento de aproximación a la percepción sobre este tipo de casos en Colombia y se considera que este punto de vista se puede enriquecer con una mayor cantidad de entrevistas tanto a fiscales del distrito como de otras regiones del país, ya que cada dirección seccional cuenta con cierta autonomía frente a las demás. Igualmente, podría haber más entrevistas a miembros del área ciberseguridad de las entidades financieras (no solo gerentes), dando así un acercamiento holístico a esta problemática.

Los comentarios recibidos por parte de los fiscales Daza y Romero destacan la importancia que ha jugado la capacitación en aspectos técnicos y de terminología para poder desempeñar de una manera más eficiente el manejo de los casos de ciberdelitos. Si bien este tema es mencionado en los documentos CONPES 3701 (identificando la ausencia de cursos y la importancia de estos) y CONPES 3854 (señalando como aumentó la oferta de cursos con respecto al 2011), se observa que se necesitan mayores esfuerzos, en específico para lograr que cada vez más fiscales, jueces e investigadores participen en este tipo de programas académicos. Asobancaria, de la mano de la Universidad de los Andes, ha brindado cursos a fiscales, investigadores y técnicos investigadores de la fiscalía desde 2016. En su última edición del año 2018, asistieron cerca de 40 participantes, tratando temas como informática jurídica, judicialización de delitos informáticos, evidencia digital, entre otros.

Del lado de la banca se percibe que el marco regulatorio ha brindado oportunidades en el manejo y tipificación de estos casos, pero ya sea por las mismas características del sistema penal o la complejidad de estos casos, el proceso de judicialización no es tan ágil como se desearía. Con base en lo anterior, políticas públicas que brinden mayor capacitación y aprendizaje en judicialización del ciberdelito para miembros de la rama judicial podría dar celeridad a estos casos, a la vez que la pronta y efectiva judicialización podría disuadir a criminales de realizar este tipo de actividades. Igualmente, la participación de la banca y de los entes reguladores es vital para que iniciativas de este tipo sean exitosas, por lo que mayores esfuerzos de cooperación entre las diferentes entidades podrían enfocarse en este aspecto.

Por otra parte, todos los entrevistados resaltan el rol que juega la educación financiera de los usuarios como herramienta para prevenir el fraude, y concuerdan en el desconocimiento por parte de los usuarios como característica recurrente al momento de tratar con denuncias. En años recientes, se ha visto cómo la ingeniería social es una de las principales modalidades de fraude, por lo que el perfilamiento del tipo de víctimas engañadas por los criminales servirá como insumo para que las campañas de educación financiera sean más efectivas. Con esto se busca que los usuarios más predispuestos a sufrir este tipo de delitos sean más conscientes en detectar fraudes y sean cuidadosos con su información financiera.

Finalmente, si bien las sugerencias anteriormente mencionadas para combatir el ciberfraude son comentarios basados en entrevistas, es evidente que este tipo de políticas públicas necesitan, para su eficiente gestión, planeación y desarrollo de la cooperación entre todos los actores del ecosistema financiero, desde los usuarios hasta los reguladores y entidades estatales. Esto es muy importante si se tiene en consideración el gran conjunto de posibilidades que trae consigo la banca digital y la transformación actual de la banca.

Agradecimientos

Desde Asobancaria la Dirección de Gestión Operativa y Seguridad agradecemos la participación de la Fiscalía General de la Nación, a los fiscales entrevistados Diana Romero y Héctor Daza, la colaboración del investigador Wilington Alvarez, a los directores de seguridad entrevistados, Gabriel Lasso, Jorge Rodríguez y Anuar Torres y a sus correspondientes entidades bancarias, a los miembros de la Organización de los Estados Americanos que permitieron esta colaboración, Barbara Marchiori De Assis y Belisario Contreras.

Referencias

• Banco Interamericano de Desarrollo & Organización de Estados Americanos (2016). Perfiles de países: Colombia, Ciberseguridad ¿Estamos preparados en América Latina y el Caribe? (p. 64), https://publications.iadb.org/en/cybersecurity-are-we-ready-latin-america-and-caribbean. Recuperado marzo 2019.

• Becker, G (1968). Crime and Punishment: An Economic Approach, The Journal of Political Economy, 76, Número 2. (Mar. -Apr. 1968), https://www.jstor.org/stable/1830482, Recuperado junio 2019.

• Council of Europe (s.f.). Details of Treaty No. 185, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185. Recuperado mayo, 2019.

• El Tiempo (2002). Los chips se toman las tarjetas, https://www.eltiempo.com/archivo/documento/MAM-1334583. Recuperado junio, 2019.

• Fondo Monetario Internacional (2018). Estimación del riesgo cibernético en el sector financiero, Diálogo a fondo, El blog del FMI sobre temas económicos de América Latina, https://blog-dialogoafondo.imf.org/?p=9460. Recuperado marzo, 2019.

• Forum of Incident Response and Security Teams (2019). FIRST Teams, https://www.first.org/members/teams/. Recuperado marzo 2019.

• International Telecommunication Unit (2017). Global Security Index (p. 52). Ginebra, Suiza.

• Kaspersky Lab (s.f.), Ingeniería social: definición. https://latam.kaspersky.com/resource-center/definitions/what-is-social-engineering. Recuperado mayo, 2019.

• Remolina, N. (2010). Anotaciones sobre la Ley 1273 de 2009. En Cano, J. (Coord.), El peritaje informático y la evidencia digital en Colombia (p. 239). Bogotá, Colombia. Ediciones Uniandes.

• Superintendencia Financiera de Colombia (2007). Octubre 2007, Circular Externa 052, https://www.superfinanciera.gov.co/publicacion/20072. Recuperado junio, 2019.

• Superintendencia Financiera de Colombia (2012). Octubre 2012, Circular Externa 042, https://www.superfinanciera.gov.co/publicacion/61268. Recuperado junio, 2019.

• Superintendencia Financiera de Colombia (2018). Circulares Externas 2018, https://www.superfinanciera.gov.co/publicacion/10096745. Recuperado Junio, 2019.

• Superintendencia Financiera de Colombia (2019). Informe de Operaciones, segundo semestre de 2018, https://www.superfinanciera.gov.co/publicacion/61066. Recuperado marzo, 2019.

A cerca de los autores:

• **Belisario Contreras**, Gerente del Programa de Ciberseguridad, Comité Interamericano contra el Terrorismo (CICTE), Organización de los Estados Americanos (OEA).

• **Jorge Bejarano**, Consultor del Programa de Ciberseguridad, Comité Interamericano contra el Terrorismo (CICTE), Organización de los Estados Americanos (OEA).

• **Orlando Garces**, Consultor del Programa de Ciberseguridad, Comité Interamericano contra el Terrorismo (CICTE), Organización de los Estados Americanos (OEA).

• **Raúl Morales Reséndiz**, Gerente de Mercados Financieros e Infraestructuras en el Centro de Estudios Monetarios Latinoamericanos (CEMLA).

• **Adam Palmer**, Jefe Global de Control y Mitigación de Riesgos de Ciberseguridad, Banco Santander.

• **Gilberto Martins de Almeida**, Abogado, Martins de Almeida Advogados.

• **José Marangunich**, Gerente de Seguridad y Prevención de Fraudes en el Banco de Crédito de Perú (BCP).

• **Jorge Castaño**, Superintendente Financiero de Colombia.

• **Sandra Rueda**, Profesora Asociada del Departamento de Ingeniería de Sistemas y Computación en la Universidad de los Andes, Colombia.

• **Mario Linares Vásquez**, Profesor Asistente de la Universidad de los Andes, Colombia.

• **Camilo Andrés Ortiz-Casas**, Estudiante de la Maestría en Seguridad de la Información en la Universidad de los Andes, Colombia.

• **Armando Colmenares Duque**, Fiscal Delegado de la Dirección del CTI de la Fiscalía General de la Nación.

• **Jaime Andres Rincon Arteaga**, Director de Gestión Operativa y Seguridad de Asobancaria.

• **Andres Quijano Diaz**, Profesional Senior de la Dirección de Gestión Operativa y Seguridad de Asobancaria.

• **María Camila Barrera Neira**, Profesional Junior de la Dirección de Gestión Operativa y Seguridad de Asobancaria.

• **Santiago Castiblanco Hernández**, Profesional Junior de la Dirección de Gestión Operativa y Seguridad de Asobancaria.

Notas a pie de página

1. Disponible en: https://www.internetworldstats.com/stats.htm

2. Minsait (2018). Tendencias en Medios de Pago 2018. Disponible en: https://www.minsait.com/sites/default/files/newsroom_documents/tendenciasmediosdepago_2018.pdf

3. Tomado de Informe Global de Riesgos 2018, http://reports.weforum.org/global-risks-2018/files/2018/01/Global-Risk-Report-2018-Executive-Summary-Spanish.pdf&embedded=true (P. 2).

4. Tomado de: http://eprints.uwe.ac.uk/38793/3/Creative%20leadership%20in%20the%20cyber%20asset%20sector%20Final.pdf "Creative leadership within the cyber asset market: An interview with Dame Inga Beale" (P. 10).

5. ASOBANCARIA. Semana Económica 2018. "Disrupción digital en los mercados financieros". Edición 1161. 6 de noviembre de 2018. Disponible en: https://www.asobancaria.com/wp-content/uploads/1161.pdf

6. Así lo ratifica el Banco Mundial en sus pronunciamientos. https://www.bancomundial.org/es/topic/financialinclusion/overview

7. https://www.un.org/sustainabledevelopment/es/objetivos-de-desarrollo-sostenible/

8. SYKES, Nathan. "Seis tendencias tecnológicas en la industria financiera en 2018". Revista Digital Open Mind. Febrero 20 de 2018. Visible en: https://www.bbvaopenmind.com/economia/economia-global/seis-tendencias-tecnologicas-en-la-industria-financiera-en-2018/

9. Ibidem.

10. Websense revela que el sector financiero sufre incidentes de seguridad un 300% más frecuentes que otras industrias. Según se extrae del Informe "2018 Financial Services Drill-Down" elaborado por Websense Security Labs™. http://www.ingecom.net/en/ns.asp?id=813&id_noticia=5

11. CAPGEMINI. 2017. "Top 10 Trend in Capital Market 2018". Consultado en: https://www.capgemini.com/wp-content/uploads/2017/11/capital-markets-trends_2018.pdf

12. ASOBANCARIA. Semana Económica 2018. "Disrupción digital en los mercados financieros". Edición 1161. 6 de noviembre de 2018. Disponible en: https://www.asobancaria.com/wp-content/uploads/1161.pdf

13. Diario El País. "La Ciberseguridad se impone en la banca". Mayo 7 de 2019. Disponible en: https://cincodias.elpais.com/cincodias/2019/05/06/mercados/1557165809_404616.html

14. Se entiende Infraestructura Crítica Cibernética como aquella infraestructura en la que se soportan servicios esenciales tanto para los ciudadanos como para los Estados

15. El Grupo de los 7, o G7, es un grupo no formal de economías avanzadas que representan más del 64% de la riqueza global. El G7 lo integran Alemania, Canadá, Estados Unidos, Francia, Italia, Japón y Reino Unido. A pesar de no tener personalidad jurídica, el G7 ha logrado establecer algunos medios técnicos de cooperación internacional.

16. Elaborado con información pública del Financial Stability Board (FSB).

17. En abril de 2009, los jefes de Estado y de Gobierno del G20 aprobaron la creación del FSB como el sucesor del Foro de Estabilidad Financiera (FSF, por sus siglas en inglés). Su principal objetivo es mejorar la cooperación entre los diversos órganos de regulación y supervisión financiera, mercados e instituciones financieras, a nivel internacional, con el fin de promover la estabilidad en el sistema financiero internacional.

18. El FSB tiene contemplado que estos lineamientos estarán listos en 2019.

19. CPMI (2016).

20. El CSP de SWIFT es un programa de controles que es obligatorio para cualquier entidad usuaria de la red. SWIFT ha establecido un monitoreo permanente del cumplimiento de los controles para todos sus usuarios, con el objetivo de asegurar que haya medidas vigentes y en práctica para que los puntos de acceso a la red internalizan medidas de seguridad cibernética. En 2017, SWIFT publicó un nuevo marco de control de seguridad para clientes (CSCF, por sus siglas en inglés), que sirve de orientación adicional acerca de las pautas de implementación del CSP. El CSCF fue actualizado en 2019, al igual que ciertos aspectos del CSP.

21. "¿Es diferente el ciberataque en América Latina comparado con el resto del mundo? Aparentemente sí. Los expertos apuntan a su carácter más rudimentario pero no por eso menos eficiente. "En los ataques que vemos en la región a veces basta con recodificar o manipular un virus de Rusia y China para hacerlo invisible a los antivirus más conocidos", afirma la responsable de un importante banco de EE.UU."(https://www.bbva.com/es/ciberdelincuencia-amenaza-banca-america-latina/, escrito el 4 de septiembre de 2017, consultado el 1.° de abril de 2019)

22. "En el caso de las entidades financieras, es importante tener en cuenta que cada empleado es un punto de contacto para atacar a la organización, por lo cual la preparación y formación de cada uno de ellos es crucial para frenar la ciberdelincuencia", señala un experto en IT." ((https://www.bbva.com/es/ciberdelincuencia-amenaza-banca-americalatina/, escrito el 4 de septiembre de 2017, consultado el 1.° de abril de 2019)

23. "La experiencia ha demostrado que cuanto más enfatiza un país la popularización acelerada de los pagos móviles, más probabilidades hay de que pierda controles financieros y viceversa. El equilibrio correcto entre esos objetivos opuestos parece depender de políticas públicas específicas, diseñadas por cada país. No obstante, el fenómeno del acceso global a la adquisición de bienes o servicios en la sociedad actual requiere el desarrollo de plataformas internacionales consistentes y eficientes. La estandarización técnica y procesal es clave para construir tales bases comunes. En este sentido, debe lograrse una nueva armonización de la infraestructura tecnológica entre los operadores de redes móviles (MNO) y los bancos, y entre los miembros de cada categoría. La convergencia de medios y las atractivas perspectivas de negocio de los pagos móviles han convertido este eje en uno aún más crucial. Los aspectos anteriores parecen indicar cómo los desafíos planteados por los pagos móviles son tanto nacionales como internacionales, y cómo la coordinación necesariamente se convertirá en el foco de las cuestiones reglamentarias legales y técnicas asociadas. (MARTINS DE ALMEIDA, GILBERTO, M-PAYMENTS IN BRAZIL: NOTES ON HOW COUNTRY BACKGROUND MAY DETERMINE TIMING AND DESIGN OF REGULATORY MODEL. Seattle: Washington Journal of Law, Technology & Arts, 2012.

24. Especialmente con respecto a las instituciones financieras, como sucede también en otras economías en desarrollo: "Con respecto al estado del entorno regulatorio, el modus operandi para las agencias, en este momento, está en ponerse al día con las demás. Las leyes y regulaciones sobre delitos cibernéticos, especialmente cuando se trata del sector financiero/bancario, no se están moviendo al mismo ritmo

que el avance tecnológico que ha tenido lugar en los últimos diez años. Cada vez más servicios y transacciones bancarias se están alejando del espacio físico de hormigón para adoptar un nuevo modelo de negocio basado en la filosofía de un cliente que obtiene acceso y utiliza sus finanzas cuando y donde quiera. La banca móvil y la transmisión inalámbrica de datos aparecen como un blanco en la mira de los delincuentes cibernéticos". ZEINAB KARAKE SHALHOUB & LUBNA AL QASIMI, CYBER LAW AND CYBER SECURITY IN DEVELOPING AND EMERGING ECONOMIES 35-36 (2010), Cheltenham, Edward Elgar, 2010, pp. 35-36, citado en MARTINS DE ALMEIDA, GILBERTO, "Electronic payments and international sales of goods: new challenges", 1.ª ed. Bogotá: Universidad Externado de Colombia, 2016, v. 01, p. 259-285.

25. "Las cifras más conservadores sitúan en casi mil millones de dólares anuales las pérdidas del sector financiero latinoamericano por deficiencias relacionadas con la ciberseguridad. Sin embargo, en muchos países de la región, el concepto de ciberdelincuencia y su combate siguen estando ausentes de las normativas nacionales, lo que dificulta un marco legal para su erradicación. Estos delincuentes han ampliado el negocio a América Latina porque ven que las infraestructuras son deficientes o inexistentes y las entidades normalmente actúan de manera reactiva, con lo cual los esfuerzos preventivos son escasos. Además, existe una gran capacidad de inventiva y creatividad (en el sentido negativo) que provoca mucho daño al cliente de banca", explica un experto de una firma de investigación." (https://www.bbva.com/es/ciberdelincuenciaamenaza-banca-america-latina/, escrito el 4 de septiembre de 2017, consultado el 1.° de abril de 2019)

26. Por ejemplo, solo 6 países latinoamericanos se han adherido al Convenio de Budapest sobre ciberdelincuencia, hasta el momento. (consulte https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures)

27. "Para continuar con el tema de los ataques a las cadenas de suministro, vale mencionar al grupo MageCart que este año, con la infección de las páginas de pago de los sitios web (entre ellos, los sitios de grandes empresas como British Airways), accedió a una enorme cantidad de datos de pago con tarjeta. Este ataque fue aun más efectivo porque los delincuentes eligieron un objetivo interesante: Magento, una de las plataformas más populares para las tiendas en línea. Aprovechando las vulnerabilidades de Magento, los delincuentes pudieron infectar docenas de sitios con una técnica que, probablemente, otros grupos adoptarán." (https://securelist.lat/ksbcyberthreats-to-financial-institutions-2019-overview-and-predictions/88201/, consultado el 1.° de abril de 2019)

28. Véase https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2018/INTERPOL-and-Banco-do-Brasil-S-A-sign-cooperation-agreement-against-cybercrime, consultado el 1.° de abril de 2019)

29. Véase https://www.cibersecurity.net.br/pf-e-febraban-renovam-parceria-contra-cibercrime/.

30. Véase https://portswigger.net/daily-swig/uruguay-govt-framework-urges-better-cybersecuritypractices y https://www.idgconnect.com/idgconnect/analysis-review/1004482/latin-americabegins-acknowledge-threats-cybercrime.

31. Véase http://www.mondaq.com/x/751016/Security/Presidential+Instructive+on+Cybersecurity y https://www.efe.com/efe/english/world/chile-s-pinera-introduces-bill-to-combatcybercrime/50000262-3793072, ambos consultados el 1.° de abril de 2019.

32. Se espera que se presenten tanto cierto nivel de superposición como algún grado de enfoque distintivo: "La ciberseguridad se ha desarrollado como un paso más holístico hacia la promoción de una Internet más segura. Su enfoque más amplio abarca implicaciones penales, civiles y administrativas, así como la cooperación público-privada, que ha atraído el interés de las autoridades gubernamentales y de los ejecutivos de gestión en todas las organizaciones. Aunque todos reconocen su naturaleza global, no todos están seguros de cómo abordarlo como tal. La Unión Europea, los Estados Unidos de América y Brasil han adoptado distintas estrategias en materia de ciberseguridad: la UE ha emitido una serie de Directivas autocontenidas, pero con un giro de colocar a la región a nivel internacional en una posición destacada en la Sociedad de la Información. Los Estados Unidos han promulgado leyes principalmente para proteger infraestructuras nacionales críticas y han dejado espacio para incluir iniciativas de inteligencia territorial y extraterritorial. Brasil ha innovado al reunir aportes de la sociedad civil antes de aprobar leyes y regulaciones, fomentando así una agenda más completa, basada en principios y un proceso más participativo y políticamente legítimo". ((MARTINS DE ALMEIDA, GILBERTO, "Cybersecurity Policy and Law Making in the EU, US and Brazil", Computer Law Review International, v. 3, p. 65-74, 2016)

33. Véase https://www.clearycyberwatch.com/2018/05/brazil-issues-new-cybersecurity-regulationregulated-financial-institutions/.

34. "Excesiva legislación impone a las empresas una carga regulatoria desproporcionada para las pequeñas y medianas empresas, e incluso puede enfrentar desafíos legales, que en últimas solo sirve para retrasar el proceso de mejora de las medidas nacionales de seguridad cibernética. Por ejemplo, en los últimos diez años, los desafíos legales incluyen haber experimentado el rechazo de la legislación de seguridad cibernética por las Cortes Supremas de Perú y Argentina. Según la FGV, las estrategias de seguridad cibernética deben ser "armonizadas" no solo con el respeto a los derechos humanos, sino también con "principios técnicos clave que han permitido la innovación en Internet, como la apertura, la universalidad y la interoperabilidad". (http://country.eiu.com/article.aspx?articleid=1725661156&Country=Haiti&topic=Economy&oid=265882010&aid=1)

35. Además de las regulaciones, como aquellas relativas a la gobernanza digital y al gobierno electrónico (que conciernen especialmente a los bancos públicos, en lo que respecta al mercado financiero), que determinan el cumplimiento equilibrado de la privacidad y las obligaciones de seguridad (por ejemplo, el Decreto de Brasil n.° 8.638/16, que estableció la llamada Política de Gobernanza Digital, para las agencias de la Administración Federal: "Art. 4° O planejamento e a execução de programas, projetos e processos relativos à governança digital pelos órgãos e pelas entidades da administração pública federal direta, autárquica e fundacional deverão observar as seguintes diretrizes: (...) III - os dados serão disponibilizados em formato aberto, amplamente acessível e utilizável por pessoas e máquinas, assegurados os direitos à segurança e à privacidade;"

36. Según lo previsto por el Proyecto Digital Mercosur, que pretendía proporcionar un diagnóstico de las asimetrías entre los países locales como una base sobre la cual construir una plataforma legal más cohesiva para la región, inclusive en lo que respecta a las políticas públicas de ciberseguridad.

37. Con amplios beneficios para otras áreas: "Dependiendo del modelo regulatorio seleccionado para un entorno determinado, la brecha social puede profundizarse, el gobierno electrónico puede ser menos efectivo, el lavado de dinero puede ser más fácil y la recaudación de impuestos y el control de divisas pueden ser más difíciles". (MARTINS DE ALMEIDA, GILBERTO. "M-Payments in Brazil: Notes on How Country Background May Determine Timing and Design of Regulatory Model", Seattle: Washington Journal of Law, Technology & Arts, 2012).

38. "Si en un principio sus ataques se dirigían principalmente a los PC (en los inicios de la banca online), no han tardado

en apuntar su artillería contra el smartphone, el dispositivo de comunicación por excelencia en esta nueva era. "Los delincuentes siempre irán donde está la información y hoy en día, pocas cosas guardan más información que un móvil", afirmaba uno de los expertos de una agencia de inteligencia." (https://www.bbva.com/es/ciberdelincuenciaamenaza-banca-america-latina/, escrito el 4 de septiembre de 2017, consultado el 1.° de abril de 2019)

39. "A pesar de todo esto, comenzaremos la revisión con una tendencia positiva: en 2018, las fuerzas policiales arrestaron a varios miembros del reconocido grupo de ciberdelincuencia responsable de Carbanak/Cobalt y Fin7, entre otros. Estos grupos han participado en ataques a docenas, si no cientos, de empresas e instituciones financieras en todo el mundo. Desafortunadamente, el arresto de los miembros del grupo, entre los que se encontraba el líder de Carbanak, no logró detener por completo sus actividades. De hecho, fue el inicio del proceso de división de los grupos en unidades más pequeñas." (https://securelist.lat/ksb-cyberthreats-tofinancial-institutions-2019-overview-and-predictions/88201/, consultado el 1.° de abril de 2019)

40. "Se espera ver más malvertising, el cual se encarga de propagar el *malware*, o programa malicioso, a través de redes de anuncios online y páginas web, que ponen en relieve mayores problemas en todo el ecosistema publicitario." (https://revistamomento.com.mx/ciberdelincuencia-financiera/, consultado el 1.° de abril de 2019).

41. "Una de las nuevas preocupaciones gira en torno al llamado 'Internet de las Cosas', un universo de aparatos interconectados que compartirán información -mucha información- y que promete simplificar (o complicar) la vida de los usuarios de una manera nunca vista." (https://www.bbva.com/es/ciberdelincuencia-amenaza-banca-america-latina/, escrito el 4 de septiembre de 2017, consultado el 1.° de abril de 2019).

42. "Hacia finales del año pasado, notamos que debido a la falta de madurez de sus sistemas de seguridad, el riesgo para las nuevas compañías de tecnología financiera y de cambios de criptomonedas eran mucho mayores. Estos tipos de compañías fueron el objetivo más frecuente. El ataque más creativo durante 2018, desde nuestro punto de vista, fue AppleJeus, que apuntó a los corredores de criptomonedas. En este caso, los ciberdelincuentes crearon un software especial con apariencia y funciones legítimas. No obstante, el programa también cargaba una actualización mal intencionada que resultó ser una puerta trasera. Este es un tipo nuevo de ataque, que infecta a sus objetivos través de la cadena de suministro".

43. "El actor más activo durante 2018 fue Lazarus. Este grupo está ampliando su arsenal de herramientas de forma gradual y está en la búsqueda de objetivos nuevos. Su área actual de interés incluye bancos, compañías de tecnología financiera, cambio de criptomonedas, terminales PoS y cajeros automáticos. En términos geográficos, hemos registrado intentos de infección en docenas de países, principalmente en Asia, África y América Latina." (https://securelist.lat/ksbcyberthreats-to-financial-institutions-2019-overview-and-predictions/88201/, consultado el 1.° de abril de 2019).

44. Véase https://securelist.lat/ksb-cyberthreats-to-financial-institutions-2019-overview-and-predictions/88201/, consultado el 1.° de abril de 2019.

45. Kimberly Prost, Breaking down barriers: International cooperation in combatting transnational crime (Nov. 29, 2015 12:08 P.M.), www.oas.org/juridico/mla/en/can/en_can_prost.en.html.

46. Oficina de las Naciones Unidas contra la Droga y el Delito, supra nota 34, en 19-21, 376.

47. Oficina de las Naciones Unidas contra la Droga y el Delito, supra nota 34, a los 19.

48. Oficina de las Naciones Unidas contra la Droga y el Delito, supra nota 2, en 209-210, 212.

49. Convenio sobre ciberdelincuencia del Consejo de Europa, párrafo 282; UCC en 177.

50. Ibíd. párrafo 282.

51. Convenio sobre ciberdelincuencia del Consejo de Europa, párrafo 283.

52. Ibíd. párrafo 282-83; UCC 177

53. Ibíd. párrafo 283

54. Ibíd. párrafo 290; UCC 180-181

55. Ibíd. párrafo 290

56. Convenio sobre ciberdelincuencia del Consejo de Europa, párrafo 290.

57. Ibíd. párrafo 170. "Los datos en cuestión son datos almacenados o existentes, y no incluyen datos que aún no han existido, por ejemplo datos de tráfico o datos de contenido relacionados con comunicaciones futuras". párrafo 170

58. Ibíd. párrafo 170

59. Ibíd. Art °. 18

60. Ibíd. Art °. 18(3)(a)-(c)

61. Ibíd. párrafo 178

62. Ibíd. párrafo 205

63. Ibíd. Art °. 33

64. Ibíd. párrafo 216, 295

65. Ibíd. Art °. 21

66. Ibíd. párrafo 229

67. Ibíd. Art °. 34

68. Ibíd. párrafo 228

69. Ibíd. párrafo 228 y 297

70. Patrick Breyer, Telecommunications Data Retention and Human Rights: The Compatibility of Blanket Traffic Data Retention with the ECHR, European L. J. 365 (2005) (con una introducción a la retención de datos).

71. Oficina de las Naciones Unidas contra la Droga y el Delito, Convention Against Transnational Organized Crime (2000); J.M. Smith, An International Hit Job: Prosecuting organized Crime Acts as Crimes Against Humanity, Georgetown L. J. 1118 (2009).

72. Organización de los Estados Americanos, Inter-American Convention on Mutual Assistance in Criminal Matters (1992), http://www.oas.org/juridico/english/sigs/a-55.html.

73. Convenio Europeo de Asistencia Judicial en Materia Penal del Consejo de Europa ETS 30 (1959).

74. Convenio sobre la ciberdelincuencia del Consejo de Europa (2001).

75. Tratado modelo de las Naciones Unidas sobre asistencia judicial mutua (1999); Oficina de las Naciones Unidas contra la Droga y el Delito, Legislative Guides for the Implementation of the United Nations Convention against Transnational Organized Crime 217 (2004), http://www.unodc.org/pdf/crime/legislative_guides/Legislative%20guides_Full%20version.pdf.

76. Una lista complete de acuerdos está disponible en: http://www.ag.gov.au/www/agd/agd.nsf/page/Extradition_and_mutual_assistanceRelationship_with_other_countries.

77. Organización de los Estados Americanos, Second Meeting of Ministers of Justice or of Misters or Attorney General of the American on Cybercrime, Background Documents on the Developments on Cyber Crime in the Framework of the REMJAS and the OAS (1999), http://www.oas.org/juridico/english/cybGE_IIIrep3.pdf.

78. Oana Mihaela Pop, The Principle and General Rules of the International Judicial Cooperation in Criminal Matters, AGORA International Journal of Juridical Science 160 (2008); Ellery C. Stowell, International Law: A Restatement of Principles in Conformity with Actual Practice 262 (1931); Recueil Des Cours, Collected Courses, Hague Acad. of Int'l L. 119 (Brill 1976).

79. Oficina de las Naciones Unidas contra la Droga y el Delito, supra nota 2, en 199.

80. Convenio sobre la ciberdelincuencia del Consejo de Europa, en el preámbulo

81. Ibíd. 242

82. Ibíd. 243

83. Ibíd. 243; "Sin embargo, debe observarse que los Artículos 24 (Extradición), 33 (Asistencia mutua respecto a la recopilación en tiempo real de datos de tráfico) y 34 (Asistencia mutua en relación con interceptación de datos de contenido) les permite a las Partes prever un ámbito de aplicación diferente de estas medidas."

84. Ibíd. 244

85. Ibíd. 244

86. Ibíd. en 253

87. Ibíd. Art °. 25 párrafo 3

88. Ibíd. 256. "Los datos informáticos son altamente volátiles. Mediante unas pocas opresiones de teclas o mediante la operación de programas automáticos se puede eliminar, haciendo imposible conectar un delito con su autor o destruyendo la prueba crítica de culpabilidad. Algunas formas de datos informáticos se almacenan solo por cortos períodos de tiempo antes de ser eliminados. En otros casos, se pueden producir daños significativos a personas o bienes si la evidencia no se recopila rápidamente".

89. Véase Convenio sobre ciberdelincuencia del Consejo de Europa.

90. Cybersecurity Ventures: https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

91. "Ninth annual EY/IIF Global Bank Risk Management Survey" https://www.ey.com/Publication/vwLUAssets/ninth-annual-ey-iif-global-bank-risk-management-survey/$FILE/ninth-annual-ey-iif-global-bank-risk-management-survey.pdf

92. https://blog.es.logicalis.com/seguridad/petya-60-paises-afectados-por-el-ultimo-ciberataque-con-ransomware

93. Inglaterra al salir de la Unión Europea tiene un proyecto de ley ad-hoc "Data Protection Bill" que contiene el GDPR de la EU con cambios menores referentes a temas periodísticos y de investigación científica.

94. https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

95. Breach Level Index

96. WEF. Innovation-Driven Cyber-Risk to Customer Data in Financial Services, 2017

97. ITU. ICT Statistics, 2017.

98. HKMA. Cybersecurity Fortification Initiative, 2016

99. Perfiles de riesgo del Índice ALA de Basilea

100. Un corredor de pagos se refiere a una secuencia de bancos en una cadena de pagos, es decir, el banco destinatario/remitente, el banco receptor/el propietario de la Cuenta Nostro y el banco beneficiario.

101. Transferencia de crédito de cliente único MT103

102. SWIFT observó el uso de un MT202 en un caso aislado y el uso de MT202COV en algunos casos, cubriendo MT103 fraudulentos.

103. Estado de la ciberseguridad en el sector bancario en América Latina y el Caribe. Organización de los Estados Americanos. 2018. Disponible en: http://www.oas.org/es/sms/cicte/sectorbancariospa.pdf.

104. Financial Stability Board. Summary Report of Financial Sector Cybersecurity Regulations, Guidance and Supervisory Practices. Octubre de 2017. Disponible en: https://www.fsb.org/wp-content/uploads/P131017-1.pdf.

105. Fondo Monetario Internacional. Antoine Bouveret. Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment. Junio 2018. Disponible en: http://www.imf.org/~/media/Files/Publications/WP/2018/wp18143.ashx.

106. Ciberseguridad. ¿Estamos preparados en América Latina y el Caribe? Organización de los Estados Americanos. Banco Interamericano de Desarrollo. 2016. Disponible en: https://publications.iadb.org/publications/spanish/document/Ciberseguridad-%C2%BFEstamos-preparados-en-Am%C3%A9rica-Latina-y-el-Caribe.pdf

107. Ibíd. Pág. 64.

108. Este documento atendió las recomendaciones de varios organismos multilaterales involucrados en el análisis de aspectos de seguridad digital, tales como la Organización para la Cooperación y el Desarrollo Económicos (OCDE), la Organización de los Estados Americanos (OEA), la Organización del Tratado del Atlántico Norte (OTAN) y el Consejo Mundial de la Industria de Tecnologías de la Información (ITI, por sus siglas en inglés).

109. De conformidad con las definiciones incorporadas en el documento Conpes 3854 son múltiples las partes interesadas, el Gobierno Nacional y los territoriales, las organizaciones públicas y privadas, la Fuerza Pública, los propietarios u operadores de las infraestructuras críticas cibernéticas nacionales, la academia y la sociedad civil, quienes dependen del entorno digital para todas o algunas de sus actividades, económicas y sociales, y quienes pueden ejercer distintos roles y tener distintas responsabilidades.

110. •Delitos que tienen a la tecnología como fin: son aquellos que atentan contra la confidencialidad, integridad o disponibilidad de la información. Por ejemplo, el daño informático, el acceso ilícito a un sistema, etc. •Delitos que tienen a la tecnología como medio: se refiere a delitos ya conocidos, que se cometen a través de un sistema informático. Son delitos comunes, que ya se encuentran tipificados en la mayoría de las legislaciones, ampliados a los medios digitales. Por ejemplo, el fraude informático o la falsificación de datos digitales. •Delitos relacionados con el contenido: establece como delitos diversos aspectos de la producción, posesión y distribución electrónica de pornografía infantil. •Delitos

relacionados con infracciones a la propiedad intelectual: se refiere a la reproducción y difusión en Internet de contenido protegido por derechos de autor, sin la debida autorización. Por ejemplo: infracciones a la propiedad intelectual, piratería, etc.

111. Nota de prensa disponible en: http://www.anterior.banxico.org.mx/inicio/banner/informacion-importante-sobre-la-situacion-del-spei/%7B022CD9D7-11A9-68E6-D1A5-965F57A23F60%7D.pdf

112. El texto completo de la Circular Externa 007 de 2018 puede ser consultada a través de la página web https://www.superfinanciera.gov.co/inicio/circulares-externas-2018_10096745.

113. Comité de Supervisión Bancaria de Basilea. Taller 6 Ciberseguridad y resiliencia operacional, noviembre. Disponible en: https://www.bis.org/bcbs/events/icbs20/ws6_es.pdf

114. Comité de Supervisión Bancaria de Basilea. Cyber-resilience: Range of practices. Diciembre 2018. Disponible en: https://www.bis.org/bcbs/publ/d454.pdf.

115. Véase G20, Communiqué: G20 Finance Ministers and Central Bank Governors Meeting, Baden-Baden, Germany, 17-18 Marzo 2017. Disponible en: http://www.bundesfinanzministerium.de/Content/EN/Standardartikel/Topics/Featured/G20/g20- communique.pdf?__blob=publicationFile&v=3.

116. Fondo Monetario Internacional. Informe sobre la estabilidad financiera mundial. Octubre 2017. Disponible en: https://www.imf.org/es/Publications/GFSR/Issues/2017/09/27/global-financial-stability-report-october-2017.

117. Op. cit.

118. Banco Central Europeo. Banking Supervision: Risk Assessment for 2019. Disponible en: https://www.bankingsupervision.europa.eu/ecb/pub/pdf/ra/ssm.ra2019.en.pdf

119. Asociación de Supervisores Bancarios de las Américas. Una perspectiva general de Fintech: sus beneficios y riesgos. 2017.

120. Superintendencia Financiera de Colombia. Marzo 2019. Disponible en https://www.superfinanciera.gov.co/descargas/institucional/pubFile1036193/2019riesgosemergentesprioridadessupervision.pdf.

121. El Centro de Investigaciones Pew es una entidad políticamente independiente que investiga e informa al público sobre problemáticas, actitudes y tendencias que transforman el mundo.

122. De acuerdo con el Boletín trimestral de MinTIC, el Acceso por Suscripción "Corresponde al acceso a internet móvil a través de la contratación de un plan con cargo fijo que se paga de forma periódica. El acceso a internet debe tener en cuenta la definición establecida en el Artículo 1.3 del Título I o aquella que la modifique, adicione o sustituya, es decir, no se deben considerar accesos que únicamente hagan uso de redes privadas (...)".

123. De acuerdo con el Boletín trimestral de MinTIC, el Acceso por Demanda "Corresponde al acceso a internet móvil sin que medie la contratación de un plan para tal fin. El acceso a internet debe tener en cuenta la definición establecida en el Artículo 1.3 del Título I o aquella que la modifique, adicione o sustituya, es decir, no se deben considerar accesos que únicamente hagan uso de redes privadas (...)".

124. http://bfr.nrb.org.np/List_Banks_n_Non_Banks.php

125. https://www.siddharthabank.com:444/Branchless-Banking/169/

126. https://rbi.org.in/CommonPerson/english/scripts/banksinindia.aspx

127. https://www.unionbankofindia.co.in/english/rabd-finance-branchless-banking.aspx

128. https://www.centralbank.ae/en/financial-institutions/Commercial%20Banks

129. https://www.dibpak.com/index.php/branchless-banking

130. https://www.revolut.com/es-ES/

131. https://n26.com/en-de/

132. https://www.mintic.gov.co/portal/604/w3-article-51418.html. Consultado en mayo de 2019.

133. https://www.forossemana.com/evento/id/32157/el_futuro_de_la_industria_fintech_en_colombia. Consultado en mayo de 2019.

134. https://www.colombiafintech.co/. Consultado en mayo de 2019.

135. Parte de un sistema de cómputo transparente para el usuario que se encarga del procesamiento y almacenamiento de los datos.

136. https://www.bnamericas.com/en/news/mexican-fintech-law-raising-eyebrows-abroad

137. https://www.bnamericas.com/en/news/fintech-regulations-chile-follows-mexicos-lead1

138. https://www.bnamericas.com/en/news/brazil-to-implement-sandbox-model-for-fintech-insurtech-regulation

139. http://www.cvm.gov.br/noticias/arquivos/2019/20190613-1.html

140. https://developer.android.com/topic/performance/vitals

141. https://firebase.google.com/docs/test-lab

142. https://developer.apple.com/app-store/review/guidelines/#performance

143. https://developer.android.com/studio/publish/app-signing

144. El Convenio de Budapest es el primer tratado internacional de crímenes cometidos vía internet y otras redes informáticas, ocupándose particularmente de infracciones a los derechos de autor, fraude cibernético, pornografía infantil y violaciones a redes de seguridad. En este sentido, busca una política criminal común contra el ciberdelito, especialmente mediante adopción de legislación apropiada y fomento a la cooperación internacional.

145. Computer Security Incident Response Team, Equipo de Respuesta ante Incidencias de Seguridad Informáticas.

146. La ingeniería social es un conjunto de técnicas que usan los cibercriminales para engañar a los usuarios incautos para que les envíen datos confidenciales, infecten sus computadoras con *malware* o abran enlaces a sitios infectados.

DESAFÍOS DEL RIESGO CIBERNÉTICO EN EL SECTOR FINANCIERO PARA COLOMBIA Y AMÉRICA LATINA

DESAFÍOS DEL RIESGO CIBERNÉTICO EN EL SECTOR FINANCIERO PARA COLOMBIA Y AMÉRICA LATINA

DESAFÍOS DEL RIESGO CIBERNÉTICO EN EL SECTOR FINANCIERO PARA COLOMBIA Y AMÉRICA LATINA