Banca & Economía
2020
Edición 1256

Impacto económico y social del *phishing* y el *smishing* en Colombia y el mundo

• El 2020 ha sido, sin duda, un año lleno de cambios en muchos aspectos de la cotidianidad, principalmente en lo que concierne a la virtualidad y las tecnologías de la información y las comunicaciones. La pandemia forzó a las personas a acercarse, conocer, entender y adaptarse al uso de las tecnologías que nos rodean.

• Esta nueva forma de vida ha traído consigo innumerables beneficios y facilidades en nuestro día a día. Sin embargo, también implica una serie de responsabilidades para hacer buen uso de las tecnologías de la información y comunicaciones, con el fin de proteger nuestra información de criminales cibernéticos.

• El *phishing* y el *smishing* son dos modalidades de fraude por medio de las cuales los ciberdelincuentes engañan a las personas mediante un correo electrónico *(phishing)* o un mensaje de texto *(smishing),* que supuestamente llega de parte de una entidad oficial, como una entidad bancaria o la Dirección de Impuestos y Aduanas Nacionales (DIAN), entre otras, para que el usuario haga clic en el enlace que viene en el cuerpo del correo.

• La habilidad de los ciberdelincuentes para adquirir información haciéndose pasar por fuentes confiables en diferentes circunstancias es una de las principales razones por las que aún se presentan este tipo de fraudes.

• Las campañas de *phishing* y *smishing* no son un tema exclusivo de países de economías desarrolladas y las acciones jurídicas y penales contra los cibercriminales depende de los marcos legales de cada país, por lo cual la adhesión a convenios internacionales y la inclusión de estas actividades como punibles en códigos son desde luego avances importantes. No obstante, también es fundamental que los gobiernos enfoquen sus esfuerzos en comunicarle a los ciudadanos los riesgos y precauciones que deben tener en cuenta al recibir mensajes o navegar por la web, siendo este un eje central en la prevención de dichos delitos.

• Desde Asobancaria y sus entidades agremiadas proponemos la implementación de un mecanismo mediante el cual sea posible, de forma expedita, suspender los medios electrónicos que se utilizan con mayor frecuencia para la comisión de un delito, como los utilizados en la suplantación de páginas web de entidades financieras o el hurto de información confidencial o personal.

• Algunas soluciones podrían estar orientadas a la mejora en las interfaces de usuario, es decir, a dar advertencias activas y detectar automáticamente mensajes maliciosos o eliminar automáticamente estos contenidos.

• Finalmente, para combatir efectivamente el *phishing*, es necesaria la colaboración local e internacional entre las autoridades y organizaciones, así como la implementación de mecanismos liderados por entidades públicas y privadas que permitan gestionar de forma eficiente, en las primeras horas de atención, el incidente para obtener mejores resultados.

26 de octubre de 2020

Director:

Santiago Castro Gómez

ASOBANCARIA:

Santiago Castro Gómez
Presidente

Alejandro Vera Sandoval
Vicepresidente Técnico

Germán Montoya Moreno
Director Económico

Para suscribirse a nuestra publicación semanal Banca & Economía, por favor envíe un correo electrónico a bancayeconomia@asobancaria.com

Banca & Economía
2020
Edición 1256

Impacto económico y social del *phishing* y el *smishing* en Colombia y el mundo

Editor

Germán Montoya
Director Económico

Participaron en esta edición:

Jaime Rincón Arteaga
Andrés Quijano Díaz
Camila Barrera Neira
Santiago Castiblanco Hernández

El 2020 ha sido, sin duda, un año lleno de cambios en muchos aspectos de la cotidianidad, principalmente en lo que concierne a la virtualidad y las tecnologías de la información y las comunicaciones.

Aunque en los últimos diez años la sociedad ha presenciado una revolución digital y ha convivido con varios procesos automatizados, en lo corrido de este año la pandemia forzó a las personas a acercarse, conocer, entender y adaptarse al uso de las tecnologías que nos rodean.

Reuniones, compras, pagos y celebraciones virtuales, entre otras, se han convertido en la nueva normalidad y han generado un aumento en el uso de dispositivos electrónicos. De acuerdo con la prensa española, las nuevas necesidades digitales han incrementado, solo en el verano, un 200% el uso de smartphone y sus aplicaciones[1].

En Colombia, un estudio de la Cámara Colombiana de Comercio Electrónico pudo establecer que el crecimiento del comercio electrónico en el país fue de 73% entre el 5 de abril y el 3 de mayo[2].

Esta nueva forma de vida ha traído consigo innumerables beneficios y facilidades en nuestro día a día. Sin embargo, también implica una serie de responsabilidades para hacer buen uso de las tecnologías de la información y las comunicaciones, con el fin de proteger nuestra información de delincuentes cibernéticos, quienes, aprovechando la coyuntura y el mayor uso de computadores y smartphones, han sofisticado sus técnicas de engaño para poder robar información personal y financiera a los nuevos usuarios de las tecnologías.

Esta edición de Banca & Economía analiza algunos de los problemas asociados a estas técnicas de engaño, como el *phishing* y el *smishing*, y expone algunas de las

[1] Disponible en: https://www.eleconomista.es/tecnologia/noticias/10703746/08/20/Aumenta-un-200-el-uso-de-apps-durante-el-verano-debido-a-la%20pandemia.html.%20%20%20 https://www.semana.com/nacion/articulo/coronavirus-

[2] Cámara Colombiana de Comercio Electrónico. (2020). Segundo Informe: Impacto del Covid-19 sobre el comercio electrónico en Colombia. Obtenido de: https://www.mintic.gov.co/portal/604/articles-145322_impacto_covid19_comercio_electronico_colombia_u20200611.pdf

razones por las cuales estas problemáticas siguen vigentes en Colombia y en la región, así como sus implicaciones a futuro. Finalmente, presenta algunas recomendaciones que pueden contribuir a resolver este problema en el corto y mediano plazo.

Más allá de lo económico, ¿cómo afectan los delitos informáticos a las personas?

Si bien los estudios e información sobre delitos informáticos se centran y hacen énfasis en las pérdidas económicas que sufren las empresas y las personas cuando son víctimas de un ataque cibernético, es de crucial importancia conocer el impacto psicológico que estos pueden generar en las personas.

En abril del presente año, la Universidad de Portsmouth y algunas entidades gubernamentales del Reino Unido lanzaron el estudio Víctimas del uso indebido de la Computadora *(Victims of Computer Misuse),* en el cual, a partir de una serie de entrevistas a víctimas de *hackeos* o robos de información a través de medios informáticos, determinaron que los delitos informáticos tienen un impacto en las personas similar, e incluso en algunas ocasiones, peor que delitos físicos como el robo[3].

El impacto psicológico parece ser tan fuerte que algunos de los testimonios de las víctimas entrevistadas afirmaron que se sintieron con altos niveles de estrés, miedo, sin poder trabajar, sin privacidad, inclusive, que toda su vida y la de sus familias se puso en riesgo. Otros comenzaron a tener problemas de salud por el estrés y la ansiedad (Gráfico 1).

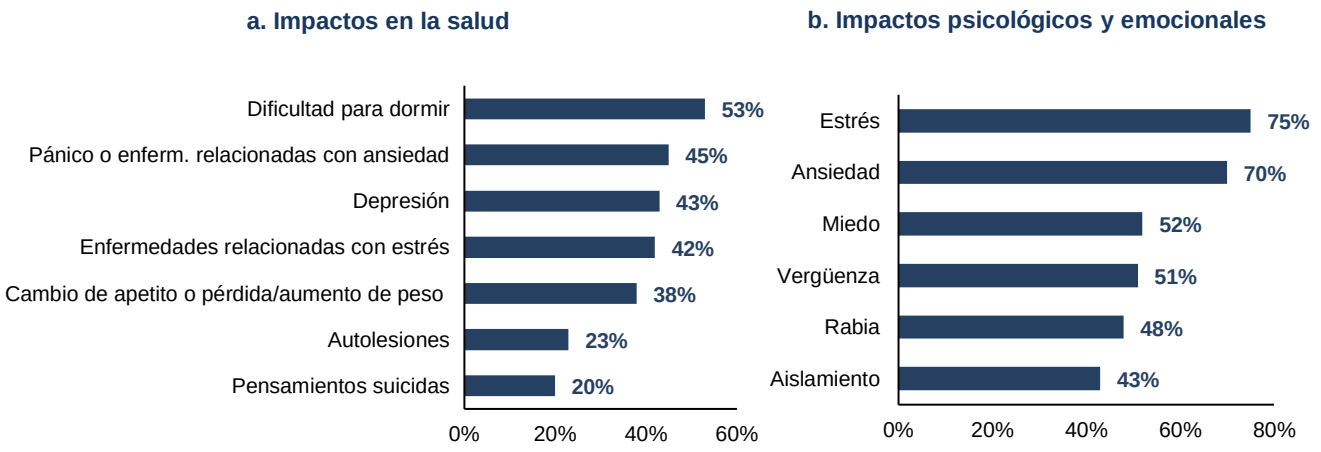
Descripción del problema en Colombia

En 2009 Colombia modificó su Código Penal e introdujo en su régimen jurídico los delitos informáticos con la Ley 1273, la cual no solo creó un bien jurídico denominado “De la protección de la información y los datos”, sino que enumeró y definió los delitos que se consideraría atentan contra la confidencialidad, integridad y disponibilidad de los datos y los sistemas informáticos.

Dentro de los delitos informáticos que enmarca la ley, se destacan:

1. Hurto por medios informáticos y semejantes: una persona manipula un sistema informático (o semejantes) y supera sus medidas de seguridad para realizar un hurto. También, cuando se suplanta a un

Gráfico 1. Impactos de los delitos informáticos en la salud mental de las personas



Fuente: Víctimas del uso indebido de la Computadora *(Victims of Computer Misuse).*

[3] Tomado de: https://www.port.ac.uk/news-events-and-blogs/news/new-home-office-funded-report-urges-greater-action-for-cybercrime-victims. Button, M., Sugiura, L., Kapend , R., Shepherd, D., Wang, V., & Blackbourn, D. (2020). Victims of Computer Misuse Main Findings.

usuario ante los sistemas de autenticación y autorización establecidos.

2. Acceso abusivo a un sistema informático: una persona sin facultades para ello accede o se mantiene en algún sistema informático que nos pertenece, esté o no protegido con medidas de seguridad.

3. Violación de datos personales: una persona sin facultades para ello y para beneficio propio o de un tercero, obtiene, sustrae, vende, envía, compra, intercepta, divulga, entre otros, códigos y datos personales contenidos en bases de datos, archivos o medios similares.

4. Suplantación de sitios web para capturar datos personales: una persona sin facultades para ello, y con fines ilícitos, diseña, desarrolla, vende o envía, entre otros, páginas electrónicas, enlaces o ventanas emergentes. Asimismo, cuando alguien engaña a un usuario para que entre a un enlace falso mientras piensa que este en el real.

5. Transferencia no consentida de activos: una persona con ánimo de lucro, por medio de manipulaciones informáticas, o semejantes, logra la transferencia no consentida de cualquier activo.

La implementación de dicha ley fue el comienzo del fortalecimiento del sistema penal colombiano en materia de delitos informáticos, y si bien con el paso de los años las entidades encargadas de investigar y lograr judicializaciones, como la Policía Nacional y la Fiscalía General de la Nación, han mejorado sus capacidades para analizar comportamientos criminales y aumentar las capturas de bandas dedicadas a crímenes cibernéticos, el país y algunos actores del ecosistema de las tecnologías de la información y las comunicaciones tienen diversos aspectos de mejora que dificultarían el actuar de los criminales.

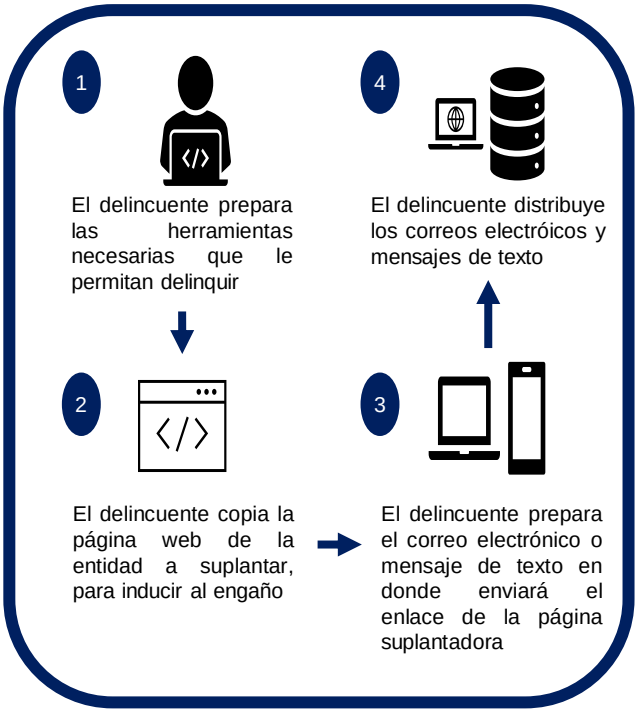
La lucha en contra del cibercrimen es una constante carrera entre las autoridades y los delincuentes, en donde estos últimos descubren una nueva forma de afectar a personas y empresas para lucrarse, lo que lleva posteriormente a la implementación de controles y barreras para hacerles frente.

Esta tarea también implica involucrar a todos los actores que directa o indirectamente están permitiendo que los delincuentes actúen de dicha forma, con el fin de cerrar brechas, mejorar la seguridad en los procesos que se vieron vulnerados y mitigar el delito.

Phishing y smishing

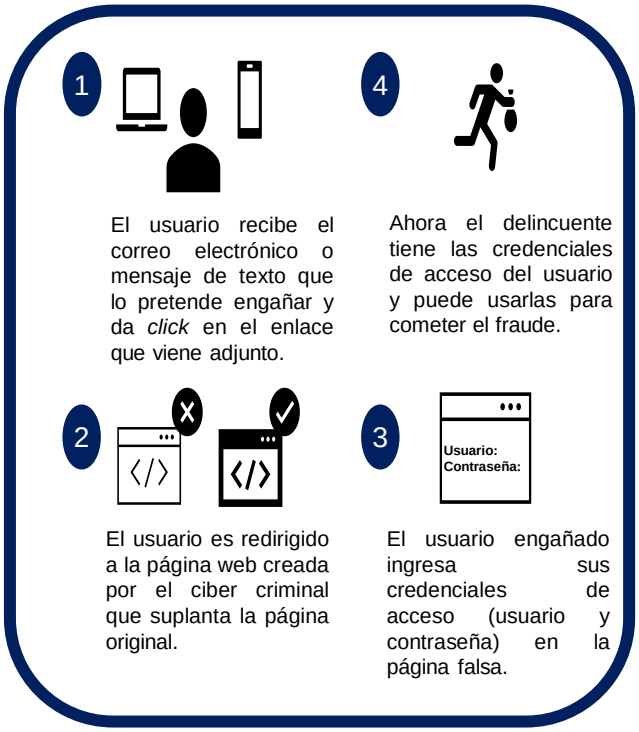
El *phishing* y el *smishing* son dos modalidades de fraude por medio de las cuales los ciberdelincuentes engañan a las personas mediante un correo electrónico (*phishing*) o un mensaje de texto (*smishing*), que supuestamente llega de parte de una entidad oficial, como una entidad bancaria o la DIAN, entre otras, para que el usuario haga clic en el enlace que viene en el cuerpo del correo o mensaje. Cuando el usuario hace clic en el enlace es redirigido a una página web que suplanta la página original de la entidad, por lo tanto, cuando la persona ingresa cualquier información en esta como usuarios y contraseñas, la información viaja directamente al ciberdelincuente

Gráfico 2. Estrategia del delincuente



Fuente: Elaboración Asobancaria

Gráfico 3. Robo y fraude al usuario



Fuente: Elaboración Asobancaria.

¿Cómo ha logrado el *phishing* perdurar en la sociedad actual?

Se considera que los primeros casos registrados de *phishing* fueron a mediados de los 90's, cuando los delincuentes enviaban mensajes haciéndose pasar por empleados de AOL (America Online) -el cual era el principal proveedor de acceso a internet en los Estados Unidos- y solicitaban datos a usuarios para verificar sus cuentas o confirmar su información de pago[4]. Desde ese entonces, el *phishing* se ha expandido a prácticamente todos los países, basándose en adquirir información de usuarios y clientes a través de mensajes (*smishing*, en caso de ser a través de SMS o mensajería instantánea) o correos fraudulentos.

La habilidad de los ciberdelincuentes para adquirir información haciéndose pasar por fuentes confiables en diferentes circunstancias es una de las principales razones por las que aún se presentan este tipo de fraudes. Ejemplo de esto son los recientes mensajes de texto y de correo electrónico falsos en la pandemia de COVID-19, en la que se hacen pasar por ministerios, secretarías de salud y otras organizaciones. El Ministerio de Salud y Protección Social de Colombia informó de correos y mensajes de Whatsapp falsos que advierten la llegada del coronavirus cerca al sector de residencia, buscando que la víctima abriera un documento adjunto que se instalaba en el dispositivo y robaba la información personal[5]. Como vemos, ya sea con supuestos mensajes de AOL o de instituciones gubernamentales, los cibercriminales han sabido detectar y explotar las circunstancias para engañar a las víctimas.

Por otra parte, la creación de nuevas herramientas, *software* o programas que se han diseñado para capturar o robar la información de los clientes sin que estos se den cuenta es otra de las razones por las que el *phishing* y *smishing* aún se presentan. El desarrollo de diferentes variantes de *malware* (término general para referirse a cualquier tipo de *software* malicioso diseñado para infiltrarse en su dispositivo sin su conocimiento[6]) no es algo exclusivo de años recientes.

En 1999, un virus denominado Melissa escaneaba la libreta de direcciones en el proveedor de correos electrónicos Outlook y enviaba copias de sí mismo a las primeras 50 direcciones encontradas, sin consentimiento del usuario, aunque los correos aparecieran firmados por este, logrando causar daños estimados en varias decenas de millones de dólares[7]. En 2004, aparece Cabir, siendo el primer gusano[8] [9] para teléfonos inteligentes, propagándose

[4] Phishing.org., History of Phishing, s.f. Recuperado de https://www.phishing.org/history-of-phishing
[5] Ministerio de Salud y Protección Social, 2020. Recuperado de https://www.minsalud.gov.co/Paginas/no-se-deje-enganar-.aspx
[6] Avast Academy, s.f. Recuperado de https://www.avast.com/es-es/c-malware
[7] Encycolpedia by Kaspersky, s.f. Recuperado de https://encyclopedia.kaspersky.es/knowledge/year-1999/
[8] Un gusano infecta un equipo, después se replica y se extiende a dispositivos adicionales, permaneciendo activo en todas las máquinas afectadas. Algunos de ellos actúan como mensajeros para instalar malware adicional.
[9] Avast Academy, s.f. Recuperado de https://www.avast.com/es-es/c-malware

a través de la red Bluetooth[10]. Finalmente, en la última década, ganaron notoriedad el troyano ZeroAccess de 2011 (que instalaba *malware via botnets*)[11] y el *ransomware* de 2017 WannaCry, que afectó a 150 países[12].

La habilidad de los cibercriminales de hacer pasar portales o interfaces por seguros para que los clientes suministren sus datos mientras un programa almacena su información, o de enviar un archivo que de ser instalado robaría datos personales y financieros, demuestra las capacidades en constante transformación con las que cuentan los cibercriminales al momento de realizar el robo de datos, ya sea a través de *spyware*, troyanos y *botnets*, entre otros.

Por último, la transformación digital y la expansión de la tecnología a varios aspectos de la economía también ha influido en que el *phishing* y *smishing* perduren en nuestros días. En 2003, se registraron sitios parecidos a plataformas como eBay y PayPal buscando engañar a clientes, mostrando el interés que comenzaron a tener los medios de pago para los ciberdelincuentes[13].

Además de estafas buscando que el cliente brindara información sobre sus tarjetas de crédito, herramientas que cada vez adquieren mayor uso por parte de clientes como son las billeteras móviles, aplicaciones en dispositivos móviles de las entidades financieras (banca móvil) o el portal bancario a través de internet, son de los principales objetivos de los cibercriminales hoy en día, enviando mensajes de texto o correos electrónicos en los que se suplanta a los establecimientos bancarios y se pide al usuario suministrar datos personales o claves de los productos que tenga con las entidades.

Cabe resaltar que cada vez es mayor el nivel de uso que han ganado este tipo de canales. En el caso colombiano, para el segundo semestre de 2019, en los canales de portal bancario y banca móvil el monto de transacciones ascendió a $1.746 billones, correspondiendo al 40,7% del total de los montos para ese período[14], por lo que los cibercriminales seguirán percibiendo como atractivos a los usuarios financieros que utilizan estas herramientas.

El *phishing* en Latinoamérica y Colombia

Las campañas de *phishing* y *smishing* no son un tema exclusivo de economías desarrolladas y las acciones jurídicas y penales contra los cibercriminales dependen de los marcos legales de cada país, por lo cual la adhesión a convenios internacionales y la inclusión en códigos de estas actividades como punibles son sin duda avances importantes. Sin embargo, también es fundamental que los gobiernos enfoquen sus esfuerzos en comunicarle a los ciudadanos acerca de los riesgos y precauciones que deben tener en cuenta al recibir mensajes o navegar por la web, siendo este un eje central en la prevención de dichos delitos. Por otra parte, la lucha contra estos delitos está fuertemente enmarcada en las leyes y códigos penales de los países.

De acuerdo con el informe *"Threat Intelligence Insider Latin America"* de Fortinet, en el segundo trimestre de este año hubo un aumento a nivel mundial en los intentos de engañar a los usuarios a ir a sitios maliciosos o de proporcionar información bajo mensajes relacionados con la pandemia actual, identificando en abril de este año más de 4.250 campañas de *phishing* relacionadas con COVID-19 por correo electrónico. Posteriormente, en los meses en mayo y junio se evidenció una notoria reducción (3.590 y 2.841 respectivamente)[15].

Según el mismo informe, México es el país donde más se detectaron amenazas de *malware* en la muestra de países, correspondiendo a un poco más de 934.000. Si bien este número corresponde al total de ataques de *software* malicioso (es decir, que no se realizaron exclusivamente a través del envío de mensajes electrónicos o de texto) la cifra da una idea del impacto que tiene este tipo de amenazas que buscan robar información o datos a clientes. Le siguen Perú, Brasil y

[10] Encycolpedia by Kaspersky, s.f. Recuperado de https://encyclopedia.kaspersky.es/knowledge/year-2004/
[11] Lifewire, A Brief History of Malware, 2019. Recuperado de https://www.lifewire.com/brief-history-of-malware-153616
[12] Avast Academy, ¿Qué es Wanna Cry?, s.f. Recuperado de https://www.avast.com/es-es/c-wannacry
[13] Phishing.org, History of phishing s.f. Recuperado de https://www.phishing.org/history-of-phishing
[14] Cálculos de Asobancaria a partir de información de la Superintendencia Financiera de Colombia.
[15] Fortinet, Thread Intelligence Insider Latin America, s.f. Recuperado de: https://www.fortinetthreatinsiderlat.com/es/Q2-2020/CO/html/trends

Colombia, con 720.193, 347.683 y 264.327 amenazas, respectivamente.

Así, el código penal mexicano señala que "a quien revele, divulgue o utilice indebidamente o en perjuicio de otro, información o imágenes obtenidas en una intervención de comunicación privada, se le aplicarán sanciones de seis a doce años de prisión y de trescientos a seiscientos días de multa"[16]. El código indica que aquellos que copien información sin autorización de equipos de informática de instituciones que integran el sistema financiero" se les impondrán de 3 meses a 2 años de prisión y de 50 a 300 días de multa"[17].

En el caso peruano, las leyes 30096 de 2013 y 30171 de 2014 indican que aquel que obtenga un provecho ilícito en perjuicio de un tercero mediante la alteración, clonación de datos o cualquier manipulación en el funcionamiento de un sistema informático será reprimido con una pena entre 3 a 8 años y con 60 a 120 días de multa[18].

En el caso colombiano, se encuentra la ley 1273 de 2009 que modificó el Código Penal y alude a los delitos contra la confidencialidad de los sistemas informáticos como el uso de *software* malicioso y violación de datos personales[19]. Así mismo, el país se encuentra adherido al Convenio de Budapest, el cual entrará en vigor en el segundo semestre de 2020.

Lo anterior resulta pertinente, toda vez que para el primer semestre de 2020 se registraron 17.211 denuncias relacionadas con delitos informáticos, con 6.650 denuncias de hurto por medios informáticos y semejantes, siendo los principales vectores de ataque el correo electrónico y los mensajes en telefonía celular[20].

Futuro del *phishing* y *smishing*

La transformación digital hace que sea más fácil no solo para las organizaciones ampliar su alcance, sino también para que los estafadores amplíen el suyo. De acuerdo con cifras del RSA, el fraude en transacciones por aplicaciones móviles ha aumentado 680% entre 2015 y 2018 a nivel mundial[21].

Es muy probable que esta tendencia de fraude a través de canales móviles se mantenga en los próximos años, teniendo en cuenta que los ciberdelincuentes siguen encontrando nuevas formas de atacar y engañar a las personas a través del *phishing* y el *malware*. Por lo tanto, en la medida en que las organizaciones continúen usando los canales móviles para ofrecer nuevos servicios digitales a sus clientes, se espera que las nuevas formas de delitos informáticos evolucionen y sean más frecuentes.

Los dispositivos móviles ocupan un lugar central como medio para cometer ciberdelitos, pero esto no significa el fin de otras modalidades de fraude que suplantan la identidad de las personas. De acuerdo con cifras del RSA, en 2018 el *phishing* representó el 47% por ciento de todos los fraudes o tipos de ataque en el mundo.

En la medida en que las organizaciones continúen introduciendo productos y servicios innovadores en línea, los ciberdelincuentes aprovecharán estos desarrollos para buscar vulnerabilidades y lanzar más ataques. Por tanto, se prevé que los mismos avances que impulsan la innovación y el crecimiento de los canales digitales sean los que incentiven a los criminales a cometer más fraudes, con lo cual la transformación digital crea tanto una oportunidad como un riesgo digital.

En 2019, el Centro de Comando Antifraude de RSA registró un aumento de los ataques de *phishing* de 178% después de que algunos bancos líderes en España lanzaron servicios de transferencias en línea, lo que indica que los ciberdelincuentes siempre están atentos ante este tipo de desarrollos para explotar sus vulnerabilidades[22].

Además de utilizar aplicaciones móviles legítimas para propósitos criminales, los ciberdelincuentes desarrollarán sus propias aplicaciones móviles para evitar su detección y ser rastreados. Este comportamiento se incrementará en la medida en que los ciberdelincuentes tengan éxito.

Con el tiempo, la amenaza de *phishing* está aumentando y se está convirtiendo en un fraude común para cometer delitos informáticos. Cada vez que los investigadores tienen alguna idea para controlar este problema, los

[16] Código Penal Federal de México, Revelación de secretos y acceso ilícito a sistemas y equipos de informática. Recuperado de https://mexico.justia.com/federales/codigos/codigo-penal-federal/libro-segundo/titulo-noveno/capitulo-i/
[17] Código Penal Federal de México, Revelación de secretos y acceso ilícito a sistemas y equipos de informática. Recuperado de https://mexico.justia.com/federales/codigos/codigo-penal-federal/libro-segundo/titulo-noveno/capitulo-ii/
[18] El Peruano, 2014. Recuperado de http://www.leyes.congreso.gob.pe/Documentos/Leyes/30096.pdf.
[19] Diario Oficial del Senado, 2009. Recuperado de http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html
[20] Centro Cibernético Policial, Comportamiento del Cibercrimen en Colombia – I Semestre 2020.
[21] Cifras tomadas de: https://www.rsa.com/content/dam/en/white-paper/2019-current-state-of-cybercrime.pdf
[22] Cifras de: 2019 CURRENT STATE OF CYBERCRIME White paper del RSA. 2019.

ciberdelincuentes cambian su estrategia de ataque explotando las vulnerabilidades encontradas en la solución actual. Los fraudes de *phishing* se pueden cometer mediante ingeniería social o mediante el uso de códigos maliciosos. En este caso, el atacante utiliza correos electrónicos falsificados o sitios web falsos para engañar a los usuarios y cometer fraude, de manera que las soluciones deben basarse en el análisis de estos esquemas.

En este sentido, las soluciones enfocadas en la creación de listas negras y listas blancas de sitios web maliciosos tienen tasas bajas de falsos positivos y son muy ineficientes para la detección de ataques de *phishing* de hora cero. Pero, concientizar y educar al usuario si se vuelve un requisito para disminuir los ataques de *phishing*.

Evolución del Internet de las Cosas

El Internet de las cosas (IoT, por sus siglas en inglés) está cambiando el estilo de vida diario de las personas, especialmente en tiempos de pandemia. Los dispositivos diseñados para ser inteligentes y estar conectados a Internet están en todas partes, en los hogares, vehículos escolares, relojes, marcapasos, etc. A pesar de estos beneficios, estos dispositivos también están facilitando el trabajo de los atacantes.

Al respecto, en IoT, el ciberdelincuente puede usar el *software* en una red de equipos infectados (*thingbots*)[23] para transmitir correos electrónicos maliciosos sin necesidad de enviar un virus o un troyano. Tales dispositivos se pueden usar fácilmente para ataques de denegación de servicio sin que el usuario lo sepa y la única forma de hacer que estos dispositivos estén libres de infecciones es desconectarlos periódicamente y actualizar su *software*.

Un ejemplo de lo anterior se dio en enero de 2015, cuando Proofpoint[24] informó de un ataque de seguridad cibernética en dispositivos de IoT en el que los correos electrónicos no deseados se enviaban de forma masiva tres veces al día y el 25% de los dispositivos eran televisores, refrigeradores y enrutadores. La misma entidad mostró en una encuesta de 2017 que durante dos semanas más de 100.000 dispositivos se vieron comprometidos para enviar más de 750.000 correos electrónicos maliciosos.

Conclusiones y consideraciones finales

De acuerdo con las cifras de la Superintendencia Financiera de Colombia, entre el 6 de abril y el 31 de agosto de 2020 (periodo de duración de la cuarentena en Colombia), el uso de canales digitales como el internet y la banca móvil aumentó un 34% y un 23,2%, respectivamente.

Teniendo en cuenta el valor de las reclamaciones por fraude y la transaccionalidad del sector, se pudo evidenciar un incremento del 10,7% del fraude en canales digitales, pasando de $0,26 por cada $10 mil transados en el período enero a agosto de 2019 a $0,29 pesos en el mismo periodo de 2020. En este sentido, el *phishing* representa el 74,2% de las reclamaciones por posible fraude y constituye la principal amenaza de seguridad para los usuarios del sistema financiero que realizan transacciones.

En septiembre del presente año el Ministerio de Tecnologías de la Información y las Comunicaciones creó una mesa de trabajo con el fin de adelantar la revisión y ajuste de los procesos técnicos necesarios a los que haya lugar con el objetivo de buscar la mejor solución para una actuación proactiva frente al fenómeno de *phishing* y *smishing* y, de esta manera, buscar soluciones conjuntas sin que se afecte el cumplimiento de la normativa vigente y se deriven así las acciones regulatorias necesarias en la materia.

Reconocemos que esta iniciativa es muy valiosa para avanzar en la detección e investigación de los delitos informáticos de los que son víctimas los ciudadanos, empresas colombianas y en particular las instituciones financieras y sus clientes. Sin embargo, esta problemática continúa exhibiendo una tendencia creciente y cada día más colombianos son víctimas de este tipo de fraudes, por

[23] Las computadoras secuestradas en una botnet convencional son conocidas como zombies o bots. David Knight, de Proofpoint, acuñó la palabra thingbot para referirse a dispositivos que no sean computadoras que han sido cooptados por una botnet. https://searchdatacenter.techtarget.com/es/definicion/IoT-botnet-botnet-de-internet-de-las-cosas

[24] Empresa de ciberseguridad que protege a las personas, los datos y las marcas de amenazas avanzadas y riesgos de cumplimiento. https://www.proofpoint.com/es/company/about

lo que se requiere combatir la cibercriminalidad con acciones más contundentes.

Desde Asobancaria y sus entidades agremiadas proponemos la implementación de un mecanismo mediante el cual se permita, de forma expedita, suspender los medios electrónicos que se utilizan con mayor frecuencia para la comisión de un delito, como los utilizados para la suplantación de páginas web de entidades financieras o el hurto de información confidencial o personal.

Adicionalmente, consideramos necesario establecer unos protocolos claros para que los proveedores de Internet (ISP's) logren bloquear aquellos contenidos que sean considerados ilegales por el uso fraudulento de marcas registradas o tengan el propósito de estafar a las personas con mensajes engañosos para obtener sus datos, proceso que podría realizarse a través de un canal seguro y ágil para que las entidades financieras y las autoridades reporten el hallazgo de una página web fraudulenta a los ISP's.

Actualmente, los proveedores de Internet tienen algunas dificultades para bloquear contenidos fraudulentos debido al principio de neutralidad en la red, el cual protege el derecho de las personas a elegir los contenidos, aplicaciones o servicios que reciben a través de internet, libre de interferencias arbitrarias por parte de los proveedores de acceso a internet. Sin embargo, la misma ley dispone que el contenido protegido por este principio debe ser lícito[25]. Por lo tanto, debe reglamentarse por parte del Gobierno Nacional la interpretación de esta Ley para declarar ilícitos los contenidos que utilicen marcas registradas de entidades financieras o cuyo propósito sea capturar información financiera de las personas.

Con respecto al *smishing*, se ha evidenciado que los proveedores de contenidos y aplicaciones (PCA) venden paquetes de códigos cortos a diferentes empresas para el envío masivo de mensajes de texto (SMS) con el fin de promocionar sus productos y servicios. Sin embargo, se ha identificado que algunas "empresas" (legalmente constituidas) adquieren estos servicios para desplegar sus ataques de *smishing* y cometer fraudes.

Si bien la Comisión de Regulación de Comunicaciones cuenta con algunos sitios web que pueden servir de apoyo en las investigaciones que realizan las autoridades para identificar a los proveedores o asignatarios de los códigos cortos de los mensajes de texto (http://www.pnn.gov.co/mapa/) y otro sitio web para obtener la información detallada de los proveedores de contenido y aplicaciones (PCA) (http://www.siust.gov.co/siust/), lo cierto es que el problema no se ha resuelto y aún existen grandes dificultades para identificar a quienes envían estos mensajes de texto masivos con contenido engañoso, así como a los propietarios de los número telefónicos desde los cuales se envían.

Por lo tanto, consideramos necesario que los PCA e ISP estudien la posibilidad de crear filtros para bloquear en tiempo y forma aquellas páginas web o mensajes de texto fraudulentos en el país.

Algunas soluciones podrían estar orientadas a la mejora en las interfaces de usuario, es decir, a dar advertencias activas y detectar automáticamente mensajes maliciosos o a eliminar de forma automática el contenido malicioso. Por ejemplo, cuando los proveedores de infraestructura detecten una palabra sospechosa puedan notificar a los usuarios acerca de los riesgos o alertas que tiene el mensaje.

Finalmente consideramos que, para combatir efectivamente el cibercrimen, es necesaria la colaboración entre las autoridades y organizaciones tanto a nivel local como internacional. Asimismo, desde Asobancaria planteamos la necesidad de implementar mecanismos liderados por entidades públicas y privadas que permitan gestionar de forma eficiente en las primeras horas de atención el incidente para obtener mejores resultados.

[25] Código Penal Federal de México, Revelación de secretos y acceso ilícito a sistemas y equipos de informática. Recuperado de https://mexico.justia.com/federales/codigos/codigo-penal-federal/libro-segundo/titulo-noveno/capitulo-i/

Colombia
Principales indicadores macroeconómicos

	2017	2018					2019*					2020*		
	Total	T1	T2	T3	T4	Total	T1	T2	T3	T4	Total	T1	T2	Total
Producto Interno Bruto**														
PIB Nominal (COP Billones)	**920,5**	230,4	236,0	251,2	268,3	**985,9**	245,4	255,0	270,6	290,7	**1061,7**	257,9	215,0	**1010,2**
PIB Nominal (USD Billones)	**308,5**	82,9	80,5	84,5	82,5	**303,4**	77,3	79,6	78,2	88,7	**324,0**	63,5	57,2	**271,3**
PIB Real (COP Billones)	**832,7**	197,4	208,1	214,7	233,5	**853,6**	203,1	214,6	222,1	241,7	**881,4**	205,9	180,8	**824,2**
PIB Real (% Var. interanual)	**1,4**	1,8	2,8	2,7	2,7	**2,5**	2,9	3,1	3,4	3,5	**3,3**	1,4	-15,7	**-6,5**
Precios														
Inflación (IPC, % Var. interanual)	**4,1**	3,1	3,2	3,2	3,2	**3,2**	3,2	3,4	3,8	3,8	**3,8**	3,7	2,9	**1,8**
Inflación sin alimentos (% Var. interanual)	**5,0**	4,3	3,8	3,8	3,7	**3,5**	3,3	3,3	3,3	3,4	**3,4**	3,3	2.02	**1,3**
Tipo de cambio (COP/USD fin de periodo)	**2984**	2780	2931	2972	3250	**3250**	3175	3206	3462	3277	**3277**	4065	3759	**3723**
Tipo de cambio (Var. % interanual)	**-0,9**	-5,5	-3,5	1,2	8,9	**8,9**	14,2	9,4	16,5	0,8	**0,8**	28,0	17,3	**14,6**
Sector Externo (% del PIB)														
Cuenta corriente	**-3,3**	-3,5	-3,9	-3,8	-4,4	**-3,9**	-4,5	-3,5	-5,0	-4,1	**-4,2**	-3,5	-3,0	**-3,3**
Cuenta corriente (USD Billones)	**-10,2**	-2,8	-3,3	-3,2	-3,7	**-13,0**	-3,5	-2,7	-4,0	-3,5	**-13,7**	-2,5	-1,7	**-4,2**
Balanza comercial	**-2,8**	-1,8	-2,6	-2,7	-3,5	**-2,7**	-3,5	-3,1	-5,0	-3,6	**-3,8**	-4,0	-4,4	**-4,2**
Exportaciones F.O.B.	**15,4**	15,8	16,4	16,2	16,4	**16,2**	16,4	17,5	15,9	15,5	**16,2**	16,0	13,8	**15,1**
Importaciones F.O.B.	**18,2**	17,7	19,1	18,9	20,0	**18,9**	19,9	20,6	20,8	19,1	**20,0**	19,9	18,3	**19,3**
Renta de los factores	**-2,7**	-3,7	-3,5	-3,4	-3,6	**-3,5**	-3,3	-3,2	-2,9	-3,3	**-3,1**	-2,5	-1,6	**-2,1**
Transferencias corrientes	**2,1**	2,0	2,2	2,3	2,7	**2,3**	2,3	2,8	2,9	2,8	**2,7**	2,9	3,1	**3,0**
Inversión extranjera directa (pasivo)	**4,4**	2,5	4,6	3,3	3,4	**3,5**	4,3	5,2	4,0	4,5	**4,4**	4,7	2,4	**3,7**
Sector Público (acumulado, % del PIB)														
Bal. primario del Gobierno Central	**-0,8**	0,0	0,1	0,0	-0,3	**-0,3**	0,0	0,9	1,4	0,4	**0,5**	...	...	**-5,9**
Bal. del Gobierno Nacional Central	**-3,6**	-0,5	-1,6	-2,4	-3,1	**-3,1**	-0,6	-0,3	-1,2	-2,5	**-2,5**	...	...	**-8,2**
Bal. estructural del Gobierno Central	**-1,9**	...	...	...	...	**-1,9**	...	...	...	...	**-1,5**	...	...	**...**
Bal. primario del SPNF	**0,5**	0,9	1,2	0,8	0,2	**0,2**	1,0	3,0	2,3	0,5	**0,5**	...	...	**-6,7**
Bal. del SPNF	**-2,7**	0,3	-0,6	-1,2	-2,9	**-2,9**	0,4	0,6	-0,5	-2,4	**-2,4**	...	...	**-9,4**
Indicadores de Deuda (% del PIB)														
Deuda externa bruta	**40,0**	38,1	38,1	38,4	39,7	**39,7**	41,6	41,5	42,0	42,7	**42,0**	47,4	49,3	**44,0**
Pública	**23,1**	22,1	21,8	21,8	21,9	**21,9**	23,1	22,6	22,6	22,7	**22,8**	25,3	26,6	**23,5**
Privada	**16,9**	16,1	16,3	16,5	17,7	**17,7**	18,5	18,9	19,5	20,0	**19,2**	22,1	22,6	**20,6**
Deuda bruta del Gobierno Central	**44,9**	43,6	45,9	47,7	49,4	**46,7**	47,4	50,6	51,9	50,3	**50,0**	59,6	...	**...**

Colombia
Estados financieros del sistema bancario

	jul-20 (a)	jun-20	jul-19 (b)	Variación real anual entre (a) y (b)
Activo	**745.004**	**755.856**	**657.433**	**11,1%**
Disponible	57.978	61.331	45.384	25,3%
Inversiones y operaciones con derivados	156.012	156.439	127.088	20,4%
Cartera de crédito	503.801	507.141	463.076	6,7%
Consumo	146.348	146.957	136.281	5,3%
Comercial	275.176	278.168	249.580	8,1%
Vivienda	69.917	69.617	64.838	5,8%
Microcrédito	12.359	12.401	12.378	-2,1%
Provisiones	32.726	32.513	28.574	12,3%
Consumo	9.923	11.341	10.329	-5,8%
Comercial	16.724	16.931	15.034	9,1%
Vivienda	2.566	2.587	2.312	8,8%
Microcrédito	1.081	1.103	899	17,9%
Pasivo	**654.254**	**665.919**	**571.729**	**12,2%**
Instrumentos financieros a costo amortizado	558.119	566.381	492.115	11,2%
Cuentas de ahorro	233.468	233.724	183.097	25,0%
CDT	169.998	166.374	161.976	2,9%
Cuentas Corrientes	69.105	72.440	55.204	22,8%
Otros pasivos	9.402	9.758	9.222	0,0%
Patrimonio	**90.750**	**89.937**	**85.704**	**3,8%**
Ganancia / Pérdida del ejercicio (Acumulada)	**3.589**	**3.124**	**5.844**	**-39,8%**
Ingresos financieros de cartera	27.481	23.685	26.645	1,1%
Gastos por intereses	9.576	8.333	9.382	0,1%
Margen neto de Intereses	18.491	15.966	18.071	0,4%
Indicadores				**Variación (a) - (b)**
Indicador de calidad de cartera	**3,83**	**3,79**	**4,67**	**-0,84**
Consumo	2,86	3,16	5,06	-2,20
Comercial	4,23	3,99	4,67	-0,45
Vivienda	3,86	3,94	3,29	0,57
Microcrédito	6,24	5,70	7,45	-1,21
Cubrimiento	**169,8**	**169,2**	**132,3**	**-37,50**
Consumo	237,4	243,8	149,9	87,55
Comercial	143,8	152,4	129,0	14,87
Vivienda	95,1	94,3	108,5	-13,36
Microcrédito	140,1	155,9	97,5	42,55
ROA	0,83%	0,83%	1,66%	-0,8
ROE	6,88%	7,07%	13,02%	-6,1
Solvencia	15,52%	14,56%	15,11%	0,4

Colombia
Principales indicadores de inclusión financiera

	2016	2017	2018	2019				2019	2020	
	Total	Total	Total	T1	T2	T3	T4	Total	T1	T2
Profundización financiera - Cartera/PIB (%) EC	**50,2**	**50,1**	**49,8**	49,5	49,6	49,9	49,8	**49,8**	51,7	…
Efectivo/M2 (%)	**12,59**	**12,18**	**13,09**	12,66	12,84	13,20	15,05	**15,05**	13,35	…
Cobertura										
Municipios con al menos una oficina o un corresponsal bancario (%)	**99,7**	**100**	**99,2**	99,7	99,7	…	99,9	**99,9**	...	...
Municipios con al menos una oficina (%)	**73,9**	**73,9**	**74,4**	74,7	74,6	74,4	74,6	**74,6**	...	...
Municipios con al menos un corresponsal bancario (%)	**99,5**	**100**	**98,3**	100	100	…	100	**100**	…	…
Acceso										
Productos personas										
Indicador de bancarización (%) SF*	**77,30**	**80,10**	81,4	82,3	82,6	83,3	82,5	**82,5**	…	…
Indicador de bancarización (%) EC**	**76,40**	**79,20**	80,5	81,3	81,6	82,4	…	**…**	…	…
Adultos con: (en millones)										
Cuentas de ahorro EC	**23,53**	**25,16**	25,75	25,79	25,99	26,3	26,6	**26,6**	…	…
Cuenta corriente EC	**1,72**	**1,73**	1,89	1,95	2,00	2,00	1,97	**1,97**	…	…
Cuentas CAES EC	**2,83**	**2,97**	3,02	3,03	3,02	3,03	3,03	**3,03**	…	…
Cuentas CATS EC	**0,10**	**0,10**	0,71	2,10	2,32	2,54	3,30	**3,30**	…	…
Otros productos de ahorro EC	**0,77**	**0,78**	0,81	0,83	0,84	0,80	0,85	**0,85**	…	…
Crédito de consumo EC	**8,74**	**9,17**	7,65	7,82	8,00	8,16	8,42	**8,42**	…	…
Tarjeta de crédito EC	**9,58**	**10,27**	10,05	10,19	10,37	10,47	10,53	**10,53**	…	…
Microcrédito EC	**3,56**	**3,68**	3,51	3,49	3,48	3,50	3,65	**3,65**	…	…
Crédito de vivienda EC	**1,39**	**1,43**	1,40	1,41	1,43	1,45	1,45	**1,45**	…	…
Crédito comercial EC	**1,23**	**1,02**	…	…	…	0,69	0,70	**0,70**	…	…
Al menos un producto EC	**25,40**	**27,1**	27,64	28,03	28,25	28,6	29,1	**29,1**	…	…
Uso										
Productos personas										
Adultos con: (en porcentaje)										
Algún producto activo SF	**66,3**	**68,6**	68,5	69,2	69,8	70,4	66,0	**66,0**	…	…
Algún producto activo EC	**65,1**	**66,9**	67,2	67,8	68,4	69,2	…	**…**	…	…
Cuentas de ahorro activas EC	**72,0**	**71,8**	68,3	68,9	70,1	70,2	70,1	**70,1**	…	…
Cuentas corrientes activas EC	**84,5**	**83,7**	85,5	85,8	85,9	85,6	85,6	**85,6**	…	…
Cuentas CAES activas EC	**87,5**	**89,5**	89,7	89,8	89,9	82,2	82,1	**82,1**	…	…
Cuentas CATS activas EC	**96,5**	**96,5**	67,7	58,2	58,3	59,0	58,3	**58,3**	…	…
Otros pdtos. de ahorro activos EC	**66,6**	**62,7**	61,2	61,3	61,8	62,0	62,8	**62,8**	…	…
Créditos de consumo activos EC	**82,0**	**83,5**	82,2	81,7	81,9	81,8	75,7	**75,7**	…	…
Tarjetas de crédito activas EC	**92,3**	**90,1**	88,7	88,3	88,6	88,0	79,5	**79,5**	…	…
Microcrédito activos EC	**66,2**	**71,1**	68,9	68,9	69,2	68,9	58,3	**58,3**	…	…

Colombia

Principales indicadores de inclusión financiera

	2016	2017	2018	2019				2019	2020	
	Total	Total	Total	T1	T2	T3	T4	Total	T1	T2
Créditos de vivienda activos EC	**79,3**	**78,9**	**77,8**	77,8	78,0	78,2	78,2	**78,2**	…	…
Créditos comerciales activos EC	**85,3**	**84,7**	**…**	…	…	61,2	45,5	**45,5**	…	…
Acceso										
Productos empresas										
Empresas con: (en miles)										
Al menos un producto EC	**751,0**	**775,2**	**946,5**	940,7	940,3	937,7	938,8	**938,8**	…	…
Cuenta de ahorro EC	**500,8**	**522,7**	**649,4**	644,3	645,0	645,4	649,1	**649,1**	…	…
Cuenta corriente EC	**420,9**	**430,7**	**502,9**	502,3	503,0	500,7	499,7	**499,7**	…	…
Otros productos de ahorro EC	**15,24**	**14,12**	**13,9**	13,8	13,9	13,1	13,8	**13,8**	…	…
Crédito comercial EC	**242,5**	**243,6**	**277,8**	278,3	279,4	284,5	285,9	**285,9**	…	…
Crédito de consumo EC	**98,72**	**102,5**	**105,8**	107,2	105,9	105,8	104,9	**104,9**	…	…
Tarjeta de crédito EC	**79,96**	**94,35**	**106,9**	109,1	109,8	111,7	113,0	**113,0**	…	…
Al menos un producto EC	**751,0**	**775,1**	**…**	…	…	…	…	**…**	…	…
Uso										
Productos empresas										
Empresas con: (en porcentaje)										
Algún producto activo EC	**74,7**	**73,3**	**71,5**	70,0	69,9	70,0	68,34	**68,34**	…	…
Algún producto activo SF	**74,7**	**73,3**	**71,6**	70,0	69,9	70,0	68,36	**68,36**	…	…
Cuentas de ahorro activas EC	**49,1**	**47,2**	**47,6**	47,3	46,9	46,7	45,8	**45,8**	....	…
Otros pdtos. de ahorro activos EC	**57,5**	**51,2**	**49,2**	49,0	50,5	50,0	52,0	**52,0**	…	…
Cuentas corrientes activas EC	**89,1**	**88,5**	**89,0**	89,3	89,5	90,2	89,7	**89,7**		
Microcréditos activos EC	**63,2**	**62,0**	**57,2**	56.6	56,6	56,1	50,3	**50,3**	…	…
Créditos de consumo activos EC	**84,9**	**85,1**	**83,9**	83,3	82,8	82,8	78,2	**78,2**		
Tarjetas de crédito activas EC	**88,6**	**89,4**	**90,2**	89,5	89,9	88,8	80,8	**80,3**	…	…
Créditos comerciales activos EC	**91,3**	**90,8**	**91,6**	83,8	80,9	81,5	77,1	**77,1**		
Operaciones (semestral)										
Total operaciones (millones)	**4.926**	**5.462**	**6.332**	-	3,952	-	4,239	**8,194**	-	3,631
No monetarias (Participación)	**48,0**	**50,3**	**54,2**	-	57,9	-	58,1	**57,9**	-	63,9
Monetarias (Participación)	**52,0**	**49,7**	**45,8**	-	42,1	-	41,9	**42,0**	-	36,0
No monetarias (Crecimiento anual)	**22,22**	**16,01**	**25,1**	-	48,6	-	29,9	**38,3**	-	31,0
Monetarias (Crecimiento anual)	**6,79**	**6,14**	**6,7**	-	19,9	-	17,6	**18,8**	-	1,3
Tarjetas										
Crédito vigentes (millones)	**14,93**	**14,89**	**15,28**	15,33	15,46	15,65	16,05	**16,05**	16,33	15,473
Débito vigentes (millones)	**25,17**	**27,52**	**29,57**	30,53	31,39	32,49	33,09	**33,09**	34,11	34,51
Ticket promedio compra crédito ($miles)	**205,8**	**201,8**	**194,4**	184,9	193,2	187,5	203,8	**203,8**	176,2	179,3
Ticket promedio compra débito ($miles)	**138,3**	**133,4**	**131,4**	118,2	116,3	114,0	126,0	**126,0**	113,6	126,0