Banca & Economía
2020
Edición 1234

Alianzas del sector público y privado para combatir el crimen financiero en tiempos del COVID-19

26 de mayo de 2020

• El mundo vive hoy un período de cambio tecnológico, geopolítico y socioeconómico sin precedentes. Para la industria de servicios financieros, este entorno crea una gran oportunidad para proporcionar servicios más rápidos, seguros y asequibles a poblaciones más grandes y diversas, pero también crea riesgos de delitos financieros que son cada vez más sofisticados y de naturaleza global.

• El fraude financiero es complejo y afecta a todo tipo de organizaciones (públicas y privadas de cualquier sector). El 47% de las empresas encuestadas alrededor del mundo presentaron, en promedio, seis incidentes de fraude en los últimos 24 meses.

• El 13 de marzo de 2020 la Interpol informó que su Unidad de Crímenes Financieros estaba recibiendo diariamente información y solicitudes por estafas y fraudes relacionados con COVID-19 por parte de los países miembro alrededor del mundo. Indicaron que a la fecha habían asistido 30 casos, bloqueado 18 cuentas bancarias y congelado alrededor de $730.000 dólares por transacciones presuntamente fraudulentas.

• La dinámica actual del cibercrimen en Colombia refleja un crecimiento gradual en el número de incidentes cibernéticos reportados a las autoridades del ecosistema de ciberseguridad. A través de los canales de atención a empresas y ciudadanos dispuestos por la Policía Nacional, se registraron 30.410 casos durante el 2019.

• Según los boletines del Centro de Capacidades para la Ciberseguridad del Centro Cibernético de la Policía Nacional, al 17 de abril del presente año se habían detectado (i) 212 noticias falsas desde la confirmación del primer caso de COVID-19 en el país, (ii) 204 páginas web con contenido malicioso (104 con *malware*, 76 con *phishing* y 24 con *spam*), de las cuales 159 fueron suspendidas, y (iii) 220 alertas que fueron generadas a través de redes sociales, prensa y canales de cooperación internacional.

• Los incidentes más reportados en Colombia siguen siendo los casos de *phishing*, con un 42%, la suplantación de identidad, con un 28%, el envío de *malware*, con 14%, y los fraudes en medios de pago en línea, con 16%.

• Combatir el crimen financiero global es, por su naturaleza, algo que ningún sector puede lograr por sí solo, por lo cual la alianza entre reguladores, fuerzas de la ley e industria privada es crítica para confrontar lo enorme y complejo de estos delitos.

• Un ejemplo reciente de la cooperación entre distintas partes para combatir el ciberfraude es la creación del COVID-19 CTI League, del cual hacen parte expertos en temas de ciberseguridad de alrededor de cuarenta países, los cuales buscan no solo combatir a *hackers* que han atacado a organizaciones de salud, sino también asesorar a proveedores de infraestructura crítica de Internet ante ataques de *phishing* con palabras relacionadas a la crisis actual.

• En Colombia se requiere la implementación de un modelo que considere las prioridades de todas las instituciones públicas y privadas y las gestione de forma eficiente en las primeras horas de atención al incidente o fraude.

Director:

Santiago Castro Gómez

ASOBANCARIA:

Santiago Castro Gómez
Presidente

Alejandro Vera Sandoval
Vicepresidente Técnico

Germán Montoya Moreno
Director Económico

Banca & Economía
2020
Edición 1234

Alianzas del sector público y privado para combatir el crimen financiero en tiempos del COVID-19

Editor

Germán Montoya
Director Económico

Participaron en esta edición:

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

Las tecnologías emergentes, así como las interconexiones entre instituciones y terceros han provocado un cambio geopolítico y socioeconómico sin precedentes. En este escenario, la industria de servicios financieros tiene una gran oportunidad para proporcionar servicios más rápidos, seguros y asequibles a poblaciones más grandes y diversas, pero también presenta nuevos riesgos de delitos financieros que son cada vez más sofisticados y de naturaleza global.

Desde que se declaró la pandemia actual, se ha evidenciado un aumento importante de actividades delincuenciales en la red y modalidades de fraude que utilizan la ingeniería social a través de correos electrónicos, mensajes de texto y llamadas. Los delincuentes están aprovechando la emergencia sanitaria mundial, el miedo y la incertidumbre para utilizar cualquier información relacionada con el COVID-19 como "señuelo" con el fin de captar la atención de la víctima, engañarla, robarle información personal o financiera y cometerle fraude.

En esta edición de Banca & Economía se exponen algunas de las modalidades de fraude que han afectado a las organizaciones desde que inició la pandemia provocada por el COVID-19, entre las que se destacan el *phishing* y el *smishing*. Así mismo, se analiza cómo algunos países han logrado diseñar estrategias para solucionar estas problemáticas a través de la cooperación público–privada. Finalmente, se recomienda lograr una coordinación más ágil y efectiva con el Gobierno Nacional para lograr mitigar los diferentes crímenes financieros que enfrentan los usuarios, especialmente en tiempos del COVID-19, en los que circula tanta información falsa y engañosa.

Panorama del fraude global y regional

La digitalización del mundo, la importancia de los datos, la anonimidad del internet, entre otros factores, han causado una constante evolución en la forma en la que los delincuentes cometen sus fraudes. Estos han desarrollado nuevas y más eficientes formas de cometer ilícitos, en las que la exposición al riesgo de ser capturado es menor y la probabilidad de éxito mayor.

Como consecuencia, las empresas del mundo están siendo cada vez más conscientes de los riesgos de robo de información o recursos a los que están expuestos, y de la

inminente posibilidad de ser víctima de algún fraude que afecte a la compañía y sus clientes.

La Encuesta Global del Crimen Económico y Fraude 2020 de Price Waterhouse Coopers (PwC)[1], que encuestó a más de 5.000 empresas alrededor del mundo acerca de su experiencia con el fraude, reveló que el 47% de las empresas encuestadas presentaron en promedio 6 incidentes de fraude en los últimos 24 meses.

De igual manera, este estudio indica que las pérdidas reportadas por fraude ascendieron a 42 billones de dólares y resalta que las pérdidas por fraudes cometidos por colaboradores de las mismas empresas o *insiders* bordearon los 100 millones de dólares. No obstante, muestra que el 39% de los fraudes se cometieron por un externo a las empresas, el 37% por un interno y el 20% cometidos en conjunto por internos y externos (Gráfico 1).

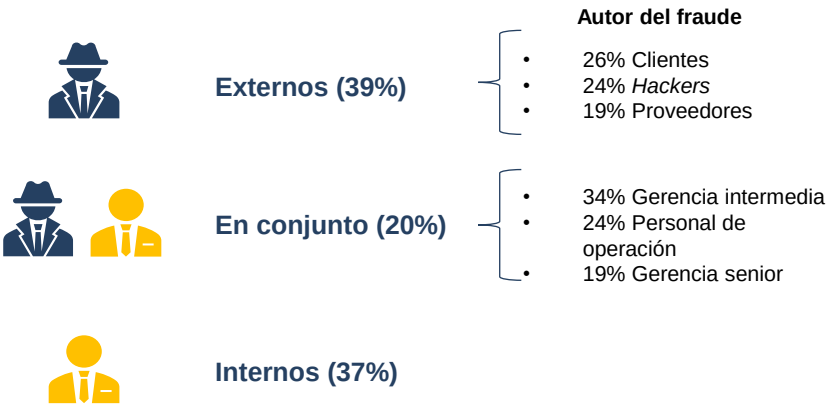
El avance del COVID-19 ha cambiado radicalmente las rutinas de las personas. Millones de empleados están trabajando ahora desde sus casas, sin acceso a sus oficinas, para prevenir la propagación del virus. Este cambio de paradigma ha tenido como consecuencia el creciente aumento en las estafas asociadas al COVID-19 en el mundo. Según el informe de KPMG sobre alertas de fraudes y estafas en tiempos de "coronavirus", algunas de las estafas relacionadas al COVID-19 incluyen[2]:

***Phishing*:** en la que defraudadores simulan ser miembros de una autoridad de salud como el Centro de Control y Prevención de Enfermedades (CDC) o la Organización Mundial de la Salud (OMS), dirigiéndose a sus víctimas a través de emails con adjuntos maliciosos o links con supuesta información sobre nuevas medidas de contención del virus, mapas del brote y actualizaciones sobre la propagación del virus, las cuales infectan los computadores y exponen la información personal como datos de tarjeta de crédito.

Estafas vía aplicaciones para celulares: los defraudadores se encuentran desarrollando o manipulando aplicaciones para celulares, las cuales externamente aparentan seguir la dispersión del COVID-19. Sin embargo, una vez instalada, la aplicación infecta el dispositivo con un malware que puede ser utilizado para obtener información personal, datos sensibles, cuentas de banco o datos de tarjetas de crédito.

Así mismo, el escenario de medidas de respuesta a la pandemia por parte de los Gobiernos, en busca de brindar beneficios y subsidios a la sociedad, ha sido aprovechado

Gráfico 1. Composición del fraude por tipo de autor



Fuente: PwC. Elaboración Asobancaria.

[1] PwC. (2020). PwC's Global Economic Crime and Fraud Survey. Obtenido de Fighting fraud: A never-ending battle: https://www.pwc.com/gx/en/forensics/gecs-2020/pdf/global-economic-crime-and-fraud-survey-2020.pdf.
[2] Información disponible en: https://assets.kpmg/content/dam/kpmg/ar/pdf/2020/covid-19-fraud-article-march-2020.pdf.

por los delincuentes para realizar sus estafas y enviar información falsa.

En Colombia, se ha detectado un incremento, particularmente, en los mensajes de texto que ofrecen beneficios o premios a raíz del Coronavirus y buscan robar las credenciales de los portales bancarios de los clientes (*smishing*). Según los más recientes boletines del Centro de Capacidades para la Ciberseguridad del Centro Cibernético de la Policía Nacional, al 17 de abril se habían detectado (i) 212 noticias falsas desde la confirmación del primer caso de Covid-19 en el país, (ii) 204 páginas web con contenido malicioso (104 con *malware*, 76 con *phishing* y 24 con *spam*), de las cuales 159 fueron suspendidas, y (iii) 220 alertas que fueron generadas a través de sus redes sociales, prensa y canales de cooperación internacional.

En el caso de América Latina, se evidencia un aumento en las modalidades de fraude que afectan a los usuarios del sistema financiero a través de plataformas digitales. Según el reporte Fraude online bancario en Latinoamérica: Una amenaza emergente, de la compañía especializada en fraude digital Buguroo[3], los delincuentes cibernéticos desplegaron en el 2018 una serie de herramientas y tácticas perversas para afectar a los bancos y sus clientes de la región.

Este tipo de dinámicas representan retos muy importantes para las entidades bancarias, considerando las tendencias en aumento de algunos tipos de modalidades cada vez más usadas. El mismo informe afirma que a diario se producen en la zona alrededor de 3,7 millones de ataques de *malware*, muchos de ellos dirigidos hacía los titulares de cuentas para robar sus credenciales y poder extraer los recursos en sus productos bancarios. El *phishing*, la sustracción de cuentas y la ingeniera social fueron otras de las modalidades de fraude que más se presentaron en 2018 según el informe.

Fraude y crimen financiero en Colombia

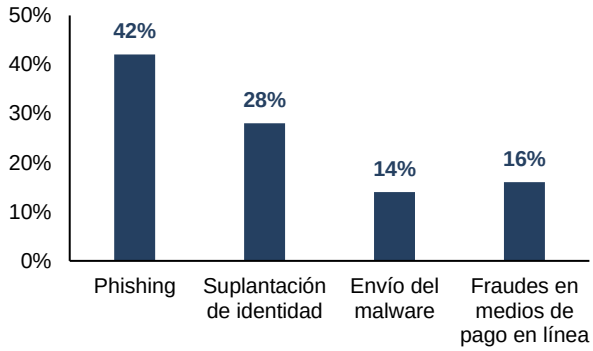
El caso colombiano no es muy lejano a lo que se observa en la región. En el país se ha evidenciado una drástica disminución en los crímenes a través de medios físicos, pero un aumento en los delitos informáticos.

Entre los delitos por medios físicos se destaca el hurto a usuarios del sistema financiero, más conocido como fleteo, y el hurto a entidades financieras (taquillazo). Mientras que, en 2011, de acuerdo con cifras de la DIJIN, se cometieron 1.700 casos de fleteo y 137 robos en las oficinas bancarias, en 2019 las cifras fueron 1.040 y 128 casos respectivamente. Por su parte, la dinámica actual de los delitos informáticos en Colombia refleja un crecimiento gradual en el número de incidentes cibernéticos reportados a las autoridades del ecosistema de ciberseguridad.

A través de los canales de atención a empresas y ciudadanos dispuestos por la Policía Nacional, se registraron 30.410 casos durante el 2019. Del total de los casos, 17.531 fueron denunciados como infracciones a la ley 1273 de 2009 por parte de las víctimas, esta cifra corresponde al 57,6% del total. Un 43% de los casos reportados en 2019, es decir, 12.879 incidentes cibernéticos, fueron gestionados sin que se llegara a instaurar una denuncia ante la Fiscalía General de la Nación.

Los incidentes más reportados en Colombia siguen siendo los casos de *phishing*, con un 42%, la suplantación de identidad, con 28%, el envío de *malware*, con 14%, y los fraudes en medios de pago en línea, con una participación del 16%[4] (Gráfico 2).

Gráfico 2. Incidentes cibernéticos reportados en Colombia – 2019



Fuente: Elaboración Asobancaria con base en las cifras del C4 de la Policía Nacional.

[3] Buguroo. (2018). Fraude online bancario en Latinoamérica: Una amenaza emergente. Obtenido de https://www.buguroo.com/es/fraude-online-bancario-en-latinoamerica-una-amenaza-emergente.
[4] Cámara Colombiana de Informática y Telecomunicaciones. (octubre de 2019). Tendencias del Cibercrimen en Colombia 2019-2020. Obtenido de https://www.ccit.org.co/estudios/tendencias-del-cibercrimen-en-colombia-2019-2020/.

Comportamiento del fraude en medio del COVID-19 y los confinamientos

Desde que se declaró la pandemia actual, se ha evidenciado un aumento importante de actividades delincuenciales en la red y modalidades de fraude que utilizan la ingeniería social a través de correos electrónicos, mensajes de texto y llamadas. Los delincuentes están aprovechando la emergencia sanitaria mundial, el miedo y la incertidumbre, para utilizar cualquier información relacionada con el COVID 19 como "señuelo" con el fin de captar la atención de la víctima, engañarla, robarle información personal o financiera y cometerle fraude.

El 13 de marzo de 2020 la Interpol informó que su Unidad de Crímenes Financieros estaba recibiendo diariamente información y solicitudes por estafas y fraudes relacionados con COVID-19 por parte de los países miembros alrededor del mundo. Indicaron que a la fecha habían asistido 30 casos, bloqueado 18 cuentas bancarias y congelado alrededor de 730.000 dólares por transacciones presuntamente fraudulentas. Entre las modalidades identificadas por el organismo destacan las estafas telefónicas, donde supuestos funcionarios de hospitales llaman a cobrar el tratamiento médico de un familiar contagiado con el virus, y correos con *phishing* y *malware*.

Además de las entidades bancarias, se están viendo afectadas por esta tendencia mundial las entidades gubernamentales e intergubernamentales, quienes están siendo suplantadas para engañar y estafar a las personas. De acuerdo con Reuters[5], en Reino Unido se realizaron llamadas a dueños de negocios para que apoyaran con 25.000 libras una iniciativa gubernamental falsa para ayudar durante la pandemia llamada “El Esquema Central de Empleadores”. Incluso la Organización de las Naciones Unidas alertó sobre comunicaciones fraudulentas suplantando su nombre.

El papel de los reguladores y creadores de política pública para mitigar el riesgo de fraude en el mundo

La cooperación entre partes es de vital importancia en los tiempos actuales, en especial si se tiene en cuenta que esta pandemia ha afectado al menos a 150 países[6]. La cooperación entre varios organismos, ya sean del sector público, sector privado, organizaciones multilaterales u organizaciones no gubernamentales, juega un rol primordial en la prevención del crimen financiero, ya sea a través de compartir anécdotas y casos de personajes clave que cuentan con gran experiencia en cada industria para adquirir saberes y técnicas, o mediante el diseño de estrategias que faciliten la articulación de los actores en caso de una futura eventualidad. Esto cobra una gran importancia en la pandemia actual de COVID-19, pues de acuerdo con Microsoft, cada país en el mundo ha tenido al menos un ciberataque con temática del coronavirus, es decir, *malware* o *phishing* que utilizan palabras relacionadas con COVID-19 para engañar al usuario (Microsoft, 2020).

Como lo señala el Foro Económico Mundial, combatir el crimen financiero global es, por su naturaleza, algo que ningún sector puede lograr por sí solo, por lo cual la alianza entre reguladores, fuerzas de la ley e industria privada es crítica para confrontar lo enorme y complejo de estos delitos[7].

Hay que resaltar, sin embargo, que la articulación entre diversos sectores no es un tema de la pandemia actual, sino el fruto de esfuerzos anteriores. Un ejemplo claro de la articulación entre sector público y privado es el desarrollo de planes de protección a la infraestructura crítica de cada país. El Departamento de Seguridad Nacional de Estados Unidos define como infraestructura crítica a todos los sistemas y activos físicos y cibernéticos que son tan vitales para la nación que su incapacidad o destrucción tendría un impacto debilitante en la salud pública, la seguridad física o la seguridad económica[8].

---

[5] Tomado de: https://uk.reuters.com/article/us-health-coronavirus-banks-fraud/banks-regulators-move-to-protect-customers-from-wave-of-coronavirus-scams-in-uk-u-s-idUKKBN21B262.
[6] Información disponible en: https://www.weforum.org/agenda/2020/01/fighting-financial-crime/.
[7] Ibídem.
[8] Información disponible en: https://www.dhs.gov/topic/critical-infrastructure-security.

Teniendo en cuenta lo anterior, proteger este tipo de infraestructura es una tarea fundamental de cooperación entre los estados y las empresas privadas, pues son estas las propietarias de la infraestructura crítica. En el caso de Estados Unidos, según Forbes[9], el 85% de las infraestructuras de sectores como defensa, energía, comunicaciones, transporte, educación y del sistema financiero es propiedad del sector privado. La cooperación entre las diversas entidades estatales y las organizaciones privadas que manejan la infraestructura crítica previene los efectos y las ganancias ilícitas de dichos ataques cibernéticos.

En el mundo, se evidencian diversas dinámicas de cooperación ante el cibercrimen. Por ejemplo, en la República de Mauricio se ha designado el National Disaster Cybersecurity and Cybercrime Committee, el cual está conformado por empresas del sector público y privado, facilitando así el monitoreo, control y toma de decisiones ante situaciones de ciber crisis a nivel nacional (ITU, 2019). Del mismo modo, en Estonia fue creada en 2018 la Estonian Information Security Association (EISA), la cual fomenta la cooperación entre la academia, el sector privado y el gobierno, buscando formalizar los vínculos actuales y aumentar las actividades de investigación y desarrollo en ciberseguridad y seguridad de la información en Estonia (ITU, 2019).

Un ejemplo reciente de la cooperación entre distintas partes para combatir el ciberfraude es la creación del COVID-19 CTI League, del cual hacen parte expertos en temas de ciberseguridad de alrededor de cuarenta países. Bajo esta iniciativa estos países buscan no solo combatir a *hackers* que han atacado a organizaciones de salud, sino también asesorar a proveedores de infraestructura crítica de Internet ante ataques de phishing con palabras relacionadas a la crisis actual, buscando así prevenir el fraude financiero[10].

Así mismo, existen alianzas y ejemplos de cooperación entre sectores en materia de prevención y lucha contra el fraude, lo que demuestra que la lucha contra el crimen financiero no solo se debe enfocar en la ciberdelincuencia sino abarcar el delito desde una visión holística.

Por su parte, la Unión Europea, que cuenta con la Oficina Europea de Lucha contra el Fraude (OLAF), utiliza su conocimiento y experiencia para ayudar a las autoridades que manejan fondos de la Unión a entender los tipos, tendencias, amenazas y riesgos del fraude, a la vez que protege los intereses financieros[11]. Esto funciona a su vez en el marco de cooperación internacional con entes investigativos, puesto que parte de los fondos de la Unión Europea son desembolsados por países y territorios no miembros de la UE a través de donaciones u otras organizaciones internacionales[12].

Teniendo en cuenta lo anterior, se evidencian los alcances y tipos de cooperación en la prevención del crimen financiero, demostrando que la lucha contra este tipo de delitos es de interés no solo de los Estados (que pueden ser afectados en las finanzas públicas) o del sector privado (que pueden ser afectados en su reputación o con pérdidas) sino de diversos actores que buscan reducir el impacto de estos crímenes en el sistema financiero nacional e internacional.

Propuestas de cooperación en Colombia para reducir el crimen financiero

El 24 de julio de 2018, el presidente de la República sancionó la Ley 1928 “por medio de la cual se aprueba el «Convenio sobre la ciberdelincuencia»”. Esto representó la adhesión de Colombia al convenio sobre cibercriminalidad de Budapest, que suponía un importante avance regulatorio para facilitar la cooperación y la judicialización del cibercrimen. Sin embargo, de acuerdo con el Global Security Index, el cual mide el compromiso de 175 países en torno a la ciberseguridad mediante la evaluación de cinco pilares (legal, técnico, organizacional, fortalecimiento de capacidades institucionales y de cooperación), Colombia pasó del puesto 46 en 2017 al puesto 73 en 2018. Esto pone en evidencia que el país

[9] Tomado de: https://www.forbes.com/sites/cognitiveworld/2019/05/06/public-private-partnerships-and-the-cybersecurity-challenge-of-protecting-critical-infrastructure/#1f3e9dff5a57.
[10] Ibídem.
[11] Información disponible en: https://ec.europa.eu/anti-fraud/policy/preventing-fraud_es.
[12] Información disponible en: https://ec.europa.eu/anti-fraud/investigations/cooperation-with-investigative-partners_es.

aún se encuentra muy rezagado en desarrollo y cumplimiento de sus objetivos de política pública en materia de seguridad digital.

En este sentido resulta fundamental que el gobierno y, específicamente, las instituciones que hacen parte del Modelo Nacional de Gestión de Incidentes, implementen acuerdos o protocolos interinstitucionales con el sector privado (especialmente el sector financiero). Estos acuerdos y protocolos resultan cruciales para trabajar de manera conjunta y coordinada en mecanismos de colaboración claros, precisos, rápidos y efectivos que permitan lograr el desmantelamiento de bandas criminales y la judicialización de sus integrantes, especialmente ahora que se evidencia un aumento en los mensajes con información falsa relacionada con la pandemia provocada por el COVID-19.

De igual manera, se debe procurar el fortalecimiento de las capacidades institucionales que se encargan de la investigación y la judicialización de estas conductas criminales. Si bien cada vez más los profesionales que imparten justicia comprenden mejor los delitos informáticos, aún falta mucho por trabajar. La evidencia digital difiere de otro tipo de pruebas físicas y, en ocasiones, se requiere de la comprensión de terminología técnica para percibir el accionar de los delincuentes.

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[13].

Oportunidades para mitigar el riesgo de *smishing* y el *phishing* en tiempos del COVID-19

Existe una modalidad de fraude que viene en aumento y que preocupa al ecosistema financiero, denominada *smishing*, que consiste en una modalidad de engaño en la cual el delincuente, a través de mensajes de texto SMS, invita a cliente a dirigirse a una página web maliciosa (por ejemplo, suplantando la de una entidad bancaria) para reclamar un supuesto premio o actualizar sus datos personales. Esta modalidad tiene el propósito de robar las credenciales y usar esta información para materializar el fraude a través de transferencias no consentidas de recursos de los productos financieros.

Actualmente los proveedores de contenidos y aplicaciones (PCA), venden paquetes de códigos cortos a diferentes empresas para el envío masivo de 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.

En el mundo, la Red de Control de Crímenes financieros (FinCEN) del Departamento del Tesoro de Estados Unidos ha identificado algunos posibles comportamientos ilícitos relacionados con COVID-19 y recomienda a las instituciones financieras que permanezcan alertas ante transacciones maliciosas o fraudulentas similares a las que ocurren después de los desastres naturales, incluidos el fraude de beneficios, el fraude de organizaciones benéficas y el fraude cibernético[14].

Para resolver esta problemática que afecta a los usuarios del sistema financiero se requiere de un esfuerzo conjunto que involucre a investigadores, proveedores de internet (ISP), operadores de telefonía móvil, bancos, reguladores de comunicaciones, áreas de vigilancia y control del MinTIC, Policía y ColCERT. Este trabajo conjunto resulta crucial para definir mecanismos de articulación que fortalezcan la cooperación, tanto en la identificación de los SMS fraudulentos, como en el diseño de estrategias de prevención que permitan filtrar estos mensajes de texto engañosos antes de que sean recibidos por sus destinatarios.

De igual manera, el *phishing* es una de las modalidades más frecuentes y con más denuncias en el país, la cual se

[13] Colmenares, 2019. "Desafíos del Riesgo Cibernético en el sector financiero para Colombia y América Latina". https://www.oas.org/es/sms/cicte/docs/Desafios-del-riesgo-cibernetico-en-el-sector-financiero-para-Colombia-y-America-Latina.pdf.
[14] Tomado de: https://www.fincen.gov/news/news-releases/financial-crimes-enforcement-network-provides-further-information-financial#_ftn5.

apalanca en el envío de correos electrónicos que dirigen a las víctimas una página web fraudulenta para estafar a los usuarios del sistema financiero por medio del robo de sus credenciales bancarias. Esto ocurre principalmente por la falta de oportunidad en el proceso de denuncia y por la dificultad para tramitar la solicitud de bloqueo de la página ante el *host* o proveedor de servicios de internet (ISP). Se ha evidenciado que mientras se surte este proceso los delincuentes continúan defraudando a los usuarios y, por ende, se pierde oportunidad en el bloqueo de estas páginas fraudulentas.

En el contexto colombiano, la Ley 1450 de 2011 estableció, en su artículo 56, el 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[15]. En este sentido, 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.

El Gobierno Nacional debe velar por la protección de los ciudadanos colombianos de una forma proactiva frente a los riesgos a que son expuestos en internet y no esperar a que ocurra el delito para frenar al delincuente. Por lo anterior, proponemos que a través del Gobierno Nacional se establezcan protocolos claros para que los ISPs bloqueen aquellos contenidos que sean considerados ilegales por el uso de marcas registradas o porque su propósito es engañar a las personas para acceder a sus datos.

Consideramos fundamental que haya una respuesta oportuna e inmediata por parte de las autoridades y de los proveedores de acceso a internet para que consideren la necesidad de crear filtros y bloquear en tiempo y forma aquellas páginas web fraudulentas en el país, especialmente en esta época donde circula tanta información falsa relacionada con el COVID-19.

Conclusiones y consideraciones finales

La llegada del COVID-19 y las medidas de aislamiento obligatorio por detener su propagación ha configurado un periodo de cambios tecnológicos, geopolíticos y socioeconómicos sin precedentes en el mundo. La dinámica de digitalización y ventas online representan grandes retos tanto para las familias como para las empresas, quienes han debido interiorizar y acoplarse gradualmente a esta nueva realidad. En particular, para la industria de servicios financieros, este entorno crea una gran oportunidad para proporcionar servicios más rápidos, seguros y asequibles a poblaciones más grandes y diversas, pero también debe enfrentarse al incremental de riesgos de delitos financieros que son cada vez más sofisticados y de naturaleza global.

En el caso de Colombia, según los boletines del Centro de Capacidades para la Ciberseguridad del Centro Cibernético de la Policía Nacional, al 17 de abril del presente año se habían detectado (i) 212 noticias falsas desde la confirmación del primer caso de COVID-19 en el país, (ii) 204 páginas web con contenido malicioso (104 con *malware*, 76 con *phishing* y 24 con *spam*), de las cuales 159 fueron suspendidas, y (iii) 220 alertas que fueron generadas a través de redes sociales, prensa y canales de cooperación internacional.

Los incidentes más reportados en Colombia siguen siendo los casos de *phishing*, con un 42%, la suplantación de identidad, con un 28%, el envío de *malware*, con 14%, y los fraudes en medios de pago en línea, con 16%.

Teniendo en cuenta que combatir el crimen financiero global es, por su naturaleza, algo que ningún sector puede lograr por sí solo, en el mundo se evidencian diversas dinámicas de cooperación ante el cibercrimen que suponen alianzas entre reguladores, fuerzas de la ley e industria privada para confrontar lo enorme y complejo de estos delitos.

Un ejemplo reciente de la cooperación entre distintas partes para combatir el ciberfraude es la creación del COVID-19 CTI League, del cual hacen parte expertos en

[15] Tomado de http://www.secretariasenado.gov.co/senado/basedoc/ley_1450_2011_pr001.html#56.

temas de ciberseguridad de alrededor de cuarenta países, los cuales buscan no solo combatir a *hackers* que han atacado a organizaciones de salud, sino también asesorar a proveedores de infraestructura crítica de Internet ante ataques de *phishing* con palabras relacionadas a la crisis actual. Así mismo, se destaca la Oficina Europea de Lucha contra el Fraude (OLAF), que utiliza su conocimiento y experiencia para ayudar a las autoridades que manejan fondos de la Unión Europea a entender los tipos, tendencias, amenazas y riesgos del fraude, a la vez que protege los intereses financieros.

En el caso de Colombia, la Ley 1928 de 2018 estableció el «Convenio sobre la ciberdelincuencia», aprobando la adhesión al convenio sobre cibercriminalidad de Budapest que suponía un importante avance regulatorio para facilitar la cooperación y la judicialización del cibercrimen. Sin embargo, aún quedan grandes retos en su implementación asociados a considerar las prioridades de todas las instituciones públicas y privadas y a gestionar de forma eficiente los casos en las primeras horas de atención al incidente o fraude, especialmente los relacionados con *phishing* y *smishing*. Así mismo, se recomienda que haya mayor claridad frente a las responsabilidades, funciones y articulación de los miembros que hacen parte del Modelo Nacional de Gestión de Incidentes (MINTIC, COLCERT, CCOCI, COORDINADOR NACIONAL DE SEGURIDAD DIGITAL y C4), cuya función principal es la articulación de las capacidades cibernéticas del Estado colombiano en el marco de un incidente informático.

Por lo anterior, es imperativo que se propenda por una coordinación más ágil y efectiva entre el Gobierno Nacional y las entidades financieras para diseñar estrategias de prevención y mitigación de los diferentes crímenes financieros que enfrentan los usuarios del sistema financiero, especialmente en tiempos del COVID-19, en los que circula tanta información falsa y engañosa y que, sin duda, marcarán en adelante una nueva realidad y grandes retos en las dinámicas de comunicación digital en el mundo.

Colombia
Principales indicadores macroeconómicos

	2016	2017	2018					2019*					2020*	
	Total	Total	T1	T2	T3	T4	Total	T1	T2	T3	T4	Total	T1	Total
Producto Interno Bruto**														
PIB Nominal (COP Billones)	**863,8**	**920,2**	231,1	234,3	248,8	264,3	**978,5**	271,8	279,5	286,4	288,9	**1126,6**	286,5	**1205,5**
PIB Nominal (USD Billones)	**287,0**	**308,4**	83,1	79,9	83,7	81,3	**301,1**	85,6	87,2	82,7	88,2	**343,8**	70,5	**305,4**
PIB Real (COP Billones)	**821,5**	**832,6**	197,7	207,8	214,9	233,5	**854,0**	203,0	214,7	222,1	241,7	**881,4**	205,2	**910,5**
PIB Real (% Var. interanual)	**2,1**	**1,4**	1,7	2,9	2,8	2,6	**2,6**	2,9	3,2	3,5	3,5	**3,3**	1,1	**3,3**
Precios														
Inflación (IPC, % Var. interanual)	**5,7**	**4,1**	3,1	3,2	3,2	3,2	**3,2**	3,2	3,4	3,8	3,8	**3,8**	3,6	**3,6**
Inflación sin alimentos (% Var. interanual)	**5,1**	**5,0**	4,1	3,8	3,7	3,5	**3,5**	3,3	3,2	3,3	3,3	**3,4**	3,3	**3,4**
Tipo de cambio (COP/USD fin de periodo)	**3010**	**2984**	2780	2931	2972	3250	**3250**	3175	3206	3462	3277	**3277**	4065	**3948**
Tipo de cambio (Var. % interanual)	**-4,4**	**-0,9**	-5,5	-3,5	1,2	8,9	**8,9**	14,2	9,4	16,5	0,8	**0,8**	28,0	**21,5**
Sector Externo (% del PIB)														
Cuenta corriente	**-4,2**	**-3,3**	-3,5	-3,9	-3,8	-4,4	**-3,9**	-4,5	-3,5	-4,9	-4,2	**-4,3**	...	**...**
Cuenta corriente (USD Billones)	**-12,0**	**-10,2**	-2,8	-3,3	-3,2	-3,7	**-13,0**	-3,5	-2,8	-4,0	-3,5	**-13,8**	...	**...**
Balanza comercial	**-4,5**	**-2,8**	-1,8	-2,6	-2,7	-3,5	**-2,7**	-3,4	-3,1	-4,9	-3,7	**-3,8**	...	**...**
Exportaciones F.O.B.	**14,8**	**15,4**	15,8	16,4	16,2	16,4	**16,2**	16,3	17,4	15,9	15,5	**16,2**	...	**...**
Importaciones F.O.B.	**19,3**	**18,2**	17,7	19,1	18,9	20,0	**18,9**	19,7	20,5	20,8	19,1	**19,9**	...	**...**
Renta de los factores	**-1,8**	**-2,7**	-3,7	-3,5	-3,4	-3,6	**-3,5**	-3,4	-3,2	-2,8	-3,4	**-3,2**	...	**...**
Transferencias corrientes	**2,1**	**2,1**	2,0	2,2	2,3	2,7	**2,3**	2,3	2,8	2,8	2,8	**2,7**	...	**...**
Inversión extranjera directa (pasivo)	**4,9**	**4,4**	2,5	4,6	3,3	3,4	**3,5**	4,3	5,2	4,0	4,4	**4,5**	...	**...**
Sector Público (acumulado, % del PIB)														
Bal. primario del Gobierno Central	**-1,1**	**-0,8**	0,0	0,1	0,0	-0,3	**-0,3**	0,0	0,9	1,4	0,4	**0,4**	...	**...**
Bal. del Gobierno Nacional Central	**-4,0**	**-3,6**	-0,5	-1,6	-2,4	-3,1	**-3,1**	-0,6	-0,3	-1,2	-2,5	**-2,5**	...	**...**
Bal. estructural del Gobierno Central	**-2,2**	**-1,9**	...	...	...	...	**-1,9**	...	...	...	...	**-1,5**	...	**...**
Bal. primario del SPNF	**0,9**	**0,5**	0,9	1,2	0,8	0,2	**0,2**	1,0	3,0	2,3	0,5	**0,5**	...	**...**
Bal. del SPNF	**-2,4**	**-2,7**	0,3	-0,6	-1,2	-2,9	**-2,9**	0,4	0,6	-0,5	-2,4	**-2,4**	...	**...**
Indicadores de Deuda (% del PIB)														
Deuda externa bruta	**42,5**	**40,0**	38,1	38,1	38,4	39,7	**39,7**	41,6	41,5	42,0	42,7	**42,0**	...	**43,7**
Pública	**25,1**	**23,1**	22,1	21,8	21,8	21,9	**21,9**	23,1	22,6	22,6	22,7	**22,8**	...	**23,3**
Privada	**17,4**	**16,9**	16,1	16,3	16,5	17,7	**17,7**	18,5	18,9	19,5	20,0	**19,2**	...	**20,4**
Deuda bruta del Gobierno Central	**44,1**	**44,9**	43,6	45,9	47,7	49,4	**46,7**	47,4	50,5	51,8	50,2	**50,0**	...	**...**

Colombia
Estados financieros del sistema bancario

	mar-20 (a)	feb-20	mar-19 (b)	Variación real anual entre (a) y (b)
Activo	**743.089**	**692.332**	**636.926**	**12,3%**
Disponible	62.030	46.509	41.435	44,2%
Inversiones y operaciones con derivados	150.918	134.860	119.811	21,3%
Cartera de crédito	504.615	487.044	451.420	7,6%
Consumo	151.328	151.010	129.809	12,3%
Comercial	271.620	254.502	246.173	6,3%
Vivienda	68.978	68.770	63.154	5,2%
Microcrédito	12.689	12.762	12.283	-0,5%
Provisiones	30.538	29.841	27.943	5,2%
Consumo	10.998	10.982	9.941	6,5%
Comercial	16.168	15.524	14.870	4,7%
Vivienda	2.461	2.444	2.235	6,0%
Microcrédito	912	891	897	-2,1%
Pasivo	**654.799**	**600.182**	**555.455**	**13,5%**
Instrumentos financieros a costo amortizado	542.119	513.776	476.438	9,6%
Cuentas de ahorro	216.213	195.535	179.218	16,2%
CDT	162.966	165.255	158.333	-0,9%
Cuentas Corrientes	77.689	61.959	54.003	38,5%
Otros pasivos	10.403	9.281	8.964	11,8%
Patrimonio	**88.290**	**92.150**	**81.471**	**4,4%**
Ganancia / Pérdida del ejercicio (Acumulada)	**2.387**	**1.636**	**2.817**	**-18,4%**
Ingresos financieros de cartera	11.905	7.872	11.236	2,0%
Gastos por intereses	4.182	2.739	3.943	2,2%
Margen neto de Intereses	8.088	5.419	7.652	1,8%
Indicadores				**Variación (a) - (b)**
Indicador de calidad de cartera	**4,30**	**4,54**	**4,79**	**-0,49**
Consumo	4,36	4,87	5,32	-0,96
Comercial	4,36	4,57	4,78	-0,41
Vivienda	3,42	3,30	3,22	0,19
Microcrédito	6,83	6,82	7,37	-0,54
Cubrimiento	**140,9**	**134,9**	**129,3**	**-11,54**
Consumo	166,5	149,4	143,9	22,64
Comercial	136,4	133,5	126,5	9,95
Vivienda	104,4	107,8	109,8	-5,41
Microcrédito	105,2	102,3	99,1	6,13
ROA	1,29%	1,63%	1,78%	-0,5
ROE	11,26%	11,67%	14,56%	-3,3
Solvencia	13,99%	14,54%	15,24%	-1,2

Colombia

Principales indicadores de inclusión financiera

	2016	2017	2018					2019				2020
	Total	Total	T1	T2	T3	T4	Total	T1	T2	T3	T4	Total	T1
Profundización financiera - Cartera/PIB (%) EC	**50,2**	**50,1**	49,7	49,7	49,2	49,8	**49,8**	49,5	49,6	49,9	49,8	**49,8**	51,7
Efectivo/M2 (%)	**12,59**	**12,18**	12,40	12,07	12,27	13,09	**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**	99,9	100	99,9	99,2	**99,2**	99,7	99,7	…	…	**…**	...
Municipios con al menos una oficina (%)	**73,9**	**73,9**	74,0	74,1	74,2	74,4	**74,4**	74,7	74,6	74,4	…	**…**	...
Municipios con al menos un corresponsal bancario (%)	**99,5**	**100**	99,9	100	98,2	98,3	**98,3**	100	100	…	…	**…**	…
Acceso													
Productos personas													
Indicador de bancarización (%) SF*	**77,30**	**80,10**	80,10	80,8	81,3	81,4	81,4	82,3	82,6	83,3	…	**…**	…
Indicador de bancarización (%) EC**	**76,40**	**79,20**	79,00	79,70	80,4	80,5	80,5	81,3	81,6	82,4	…	**…**	…
Adultos con: (en millones)													
Cuentas de ahorro EC	**23,53**	**25,16**	25,00	25,3	25,6	25,75	25,75	25,79	25,99	26,3	…	**…**	…
Cuenta corriente EC	**1,72**	**1,73**	1,74	1,81	1,8	1,89	1,89	1,95	2,00	2,00	…	**…**	…
Cuentas CAES EC	**2,83**	**2,97**	3,00	3,02	3,02	3,02	3,02	3,03	3,02	3,03	…	**…**	…
Cuentas CATS EC	**0,10**	**0,10**	0,10	0,10	0,10	0,71	0,71	2,10	2,32	2,54	…	**…**	…
Otros productos de ahorro EC	**0,77**	**0,78**	0,78	0,81	0,82	0,81	0,81	0,83	0,84	0,80	…	**…**	…
Crédito de consumo EC	**8,74**	**9,17**	7,23	7,37	7,47	7,65	7,65	7,82	8,00	8,16	…	**…**	…
Tarjeta de crédito EC	**9,58**	**10,27**	9,55	9,83	9,98	10,05	10,05	10,19	10,37	10,47	…	**…**	…
Microcrédito EC	**3,56**	**3,68**	3,41	3,50	3,49	3,51	3,51	3,49	3,48	3,50	…	**…**	…
Crédito de vivienda EC	**1,39**	**1,43**	1,34	1,37	1,38	1,40	1,40	1,41	1,43	1,45	…	**…**	…
Crédito comercial EC	**1,23**	**1,02**	0,65	0,67	0,66	…	…	…	…	0,69	…	**…**	…
Al menos un producto EC	**25,40**	**27,1**	26,8	27,2	27,5	27,64	27,64	28,03	28,25	28,6	…	**…**	…
Uso													
Productos personas													
Adultos con: (en porcentaje)													
Algún producto activo SF	**66,3**	**68,6**	67,1	68,0	68,4	68,5	68,5	69,2	69,8	70,4	…	**…**	…
Algún producto activo EC	**65,1**	**66,9**	65,7	66,6	67,1	67,2	67,2	67,8	68,4	69,2	…	**…**	…
Cuentas de ahorro activas EC	**72,0**	**71,8**	67,7	68,4	68,4	68,3	68,3	68,9	70,1	70,2	…	**…**	…
Cuentas corrientes activas EC	**84,5**	**83,7**	84,4	85,0	85,1	85,5	85,5	85,8	85,9	85,6	…	**…**	…
Cuentas CAES activas EC	**87,5**	**89,5**	89,7	89,8	89,8	89,7	89,7	89,8	89,9	82,2	…	**…**	…
Cuentas CATS activas EC	**96,5**	**96,5**	96.5	95,2	96,5	67,7	67,7	58,2	58,3	59,0	…	**…**	…
Otros pdtos. de ahorro activos EC	**66,6**	**62,7**	62,0	62,5	62,1	61,2	61,2	61,3	61,8	62,0	…	**…**	…
Créditos de consumo activos EC	**82,0**	**83,5**	82,0	81,5	81,8	82,2	82,2	81,7	81,9	81,8	…	**…**	…
Tarjetas de crédito activas EC	**92,3**	**90,1**	88,9	88,9	88,7	88,7	88,7	88,3	88,6	88,0	…	**…**	…
Microcrédito activos EC	**66,2**	**71,1**	71,2	70,4	69,4	68,9	68,9	68,9	69,2	68,9	…	**…**	…

Colombia

Principales indicadores de inclusión financiera

	2016	2017	2018					2019				2019	2020
	Total	Total	T1	T2	T3	T4	Total	T1	T2	T3	T4	Total	T1
Créditos de vivienda activos EC	**79,3**	**78,9**	78,2	77,7	77,8	77,8	77,8	77,8	78,0	78,2	…	**…**	…
Créditos comerciales activos EC	**85,3**	**84,7**	59,2	58,7	57,6	…	…	…	…	61,2	…	**…**	…
Acceso													
Productos empresas													
Empresas con: (en miles)													
Al menos un producto EC	**751,0**	**775,2**	944,3	947,8	946,6	946,5	946,5	940,7	940,3	937,7	…	**…**	…
Cuenta de ahorro EC	**500,8**	**522,7**	649,7	647,7	648,9	…	…	…	…	…	…	**…**	…
Cuenta corriente EC	**420,9**	**430,7**	488,9	505,2	502,4	…	…	…	…	…	…	**…**	…
Otros productos de ahorro EC	**15,24**	**14,12**	14,4	14,1	14,0	…	…	…	…	…	…	**…**	…
Crédito comercial EC	**242,5**	**243,6**	265,3	272,2	276,5	…	…	…	…	…	…	**…**	…
Crédito de consumo EC	**98,72**	**102,5**	104,4	106,7	105,3	…	…	…	…	…	…	**…**	…
Tarjeta de crédito EC	**79,96**	**94,35**	102,1	104,4	105,1	…	…	…	…	…	…	**…**	…
Al menos un producto EC	**751,0**	**775,1**	944,3	947,8	946,6	…	…	…	…	…	…	**…**	…
Uso													
Productos empresas													
Empresas con: (en porcentaje)													
Algún producto activo EC	**74,7**	**73,3**	71,6	71,9	71,6	...	...	…	…	…	…	**…**	…
Algún producto activo SF	**74,7**	**73,3**	71,7	71,9	71,6	71,6	71,6	70,0	69,9	70,0	…	**…**	…
Cuentas de ahorro activas EC	**49,1**	**47,2**	48,1	47,7	48,2	…	…	…	…	…	…	**…**	....
Otros pdtos. de ahorro activos EC	**57,5**	**51,2**	50,8	49,5	49,5	…	…	…	…	…	…	**…**	…
Cuentas corrientes activas EC	**89,1**	**88,5**	88,5	88,2	88,6								
Microcréditos activos EC	**63,2**	**62,0**	58,5	58,5	57,2								
Créditos de consumo activos EC	**84,9**	**85,1**	83,7	83,4	83,7	…	…	…	…	…	…	**…**	…
Tarjetas de crédito activas EC	**88,6**	**89,4**	90,6	89,8	90,0								
Créditos comerciales activos EC	**91,3**	**90,8**	91,0	91,1	91,4	…	…	…	…	…	…	**…**	…
Operaciones (semestral)													
Total operaciones (millones)	**4.926**	**5.462**	- 2.926		- 3.406		**6.332**	-	3,952	-	4,239	**8,194**	-
No monetarias (Participación)	**48,0**	**50,3**	-	52,5	-	55,6	**54,2**	-	57,9	-	58,1	**57,9**	-
Monetarias (Participación)	**52,0**	**49,7**	-	47,4	-	44,3	**45,8**	-	42,1	-	41,9	**42,0**	-
No monetarias (Crecimiento anual)	**22,22**	**16,01**	- 18,66		-	30,9	**25,1**	-	48,6	-	29,9	**38,3**	-
Monetarias (Crecimiento anual)	**6,79**	**6,14**	-	6,30	-	7,0	**6,7**	-	19,9	-	17,6	**18,8**	-
Tarjetas													
Crédito vigentes (millones)	**14,93**	**14,89**	14,91	15,03	15,17	15,28	**15,28**	15,33	15,46	15,65	16,05	**16,05**	16,33
Débito vigentes (millones)	**25,17**	**27,52**	28,17	28,68	29,26	29,57	**29,57**	30,53	31,39	32,49	33,09	**33,09**	34,11
Ticket promedio compra crédito ($miles)	**205,8**	**201,8**	194,1	196,1	183,1	194,4	**194,4**	184,9	193,2	187,5	203,8	**203,8**	176,2
Ticket promedio compra débito ($miles)	**138,3**	**133,4**	121,2	123,2	120,3	131,4	**131,4**	118,2	116,3	114,0	126,0	**126,0**	113,6