# Boletín de Fraude 15 de mayo 2020

**01** Contingencia obliga a que las entidades financieras modifiquen sus servicios.

**02** UIF congela cuentas a defraudador por supuestas tarjetas de apoyos ante COVID-19.

**03** Cifras millonarias, por fraudes relacionados con Covid-19.

**04** Por Covid-19, se ha hecho mal uso del sector financiero formal: GAFI.

**05** Autoridad Bancaria Europea quiere reforzar la lucha contra los fraudes de dividendos.

**06** Ciberdelitos aumentan en la contingencia; incrementaron 14% entre marzo y abril.

## ¿HAS SIDO VÍCTIMA DE FRAUDE O AÚN NO LO SABES?

**CONTÁCTANOS**

protiviti®

*Face the Future with Confidence*

**Protiviti** líder en servicios de consultoría de riesgos de negocios y auditoría interna, apoya a la lucha antifraude.
Quincenalmente distribuimos esta recopilación de las notas más sobresalientes relacionadas con delitos de cuello blanco.

protiviti®
Face the Future with Confidence

# Contingencia obliga a que las entidades financieras modifiquen sus servicios.

La contingencia cambió algunos hábitos que los mexicanos tenían en su rutina del día a día, entre ellas la adopción o reforzamiento de las nuevas tecnologías para diversas actividades como compras, pagos o pedidos de diversos servicios a domicilio, e incluso operaciones que usualmente se realizan en las sucursales bancarias.

**03 mayo**

**2020**

**El Economista.**

En este sentido, instituciones financieras como los bancos han solicitado a sus clientes que, ante el cierre de una parte de sus sucursales opten por los canales digitales, tales como las aplicaciones para dispositivos móviles. Sin embargo, aunque hay avances en cuanto a la adopción de estos servicios, en México, durante el 2018, 78% de la población no tenía contratado el servicio de banca digital debido a que prefirió el uso de otros canales, entre ellos las sucursales y los cajeros, de acuerdo con datos de la Encuesta Nacional de Inclusión Financiera 2018.

Esto ha obligado a que tanto usuarios como entidades financieras modifiquen la forma en que operan sus actividades.

“Esta situación sólo hizo apresurar el proceso de adopción de sistemas digitales de servicios financieros por Internet. La banca en línea es de lo más usado, pero cierto sector se resistía y prefería ir al banco y no tuvieron de otra más que usarla”, destacó Héctor Sosa, uno de los fundadores de la plataforma Invierte. Gurú.

De acuerdo con el especialista, ante la emergencia que se vive por el coronavirus, muchas personas optarán y recurrirán a la interacción de diversos servicios financieros mediante nuevas plataformas que usualmente se llevan a cabo cara a cara.

Mejorar servicios y experiencias, el gran reto

A decir Sosa, tanto usuarios como entidades financieras experimentan nuevas formas de atención así como de ofrecer servicios, por lo que la contingencia fue un factor que obliga a las instituciones no sólo a mejorar o reforzar sus servicios, sino también las experiencias que otorgan a sus clientes.

“Un reto importante es la demanda que tienen. Nadie esperaba esto. Están trabajando a marchas forzadas para soportar la demanda de los servicios digitales que ya tenían y trabajan para mejorar la experiencia del usuario. Ése es el principal reto, que la experiencia de las personas al usar estos servicios sea óptima, porque ahora más que nunca lo necesitan”, aseveró.

Además, el experto agregó que el siguiente reto, después de cubrir la demanda, consistirá en incrementar la oferta de servicios para que la gente cuente con más alternativas para contratar o invertir.

protiviti®
Face the Future with Confidence

# Contingencia obliga a que las entidades financieras modifiquen sus servicios. (Continuación)

**03 mayo**

**2020**

**El Economista.**

## Fintech, aliadas en la contingencia

Héctor Sosa refirió que, ante la coyuntura que se vive, los mexicanos cuentan con diversas opciones con las que podrán realizar diversas transacciones que normalmente se hacen en sucursales, con el beneficio de ser más rápidas y hacerlas desde la comodidad de su hogar.

Por ejemplo, las fintech actualmente cumplen con la función de operar 100% en línea y con beneficios que algunas entidades tradicionales no otorgan a sus usuarios.

Entre estos, se encuentra el crowdfunding, en plataformas que le permiten contribuir con pequeñas o grandes cantidades de dinero para financiar esfuerzos e iniciativas de otras personas u organizaciones.

Otra opción son los préstamos personales inmediatos que se manejan completamente en línea y que requieren sólo una fracción del tiempo para su gestión. Aunque las transacciones son seguras, debe elegir con cuidado a la fintech para evitar los fraudes cibernéticos.

La administración de las finanzas personales ahora más que nunca se ha vuelto esencial, por lo que una alternativa que las fintech ofrecen son apps que le ayudan a administrar sus finanzas y a llevar un mejor control de lo que gasta.

protiviti®
Face the Future with Confidence

# UIF congela cuentas a defraudador por supuestas tarjetas de apoyos ante COVID-19.

La Unidad de Inteligencia Financiera (UIF) de la Secretaría de Hacienda y Crédito Público (SHCP) congeló las cuentas de un defraudador con supuestas tarjetas de apoyos emergentes por COVID-19 que habrían sido emitidas por la Secretaría de Bienestar.

**04 mayo**

**2020**

**El Financiero.**

La UIF, en coordinación con la Secretaría del Bienestar, investigó los presuntos fraudes que se estaban realizando con supuestos apoyos sociales ante la emergencia por la pandemia, una acción que se suma a la denuncia que la dependencia presentó ante la Fiscalía General de la República el pasado 30 de abril en contra de quienes resulten responsables de la distribución de tarjetas falsas.

Hace unos días la Secretaría del Bienestar informó que circulaba una noticia falsa en redes sociales en la que personas ajenas a la institución ofrecían realizar por internet el trámite de supuestas tarjetas alimentarias.

“Hoy se tiene conocimiento de que, en el estado de Chiapas, los presuntos defraudadores escalaron su estrategia visitando los hogares de las y los mexicanos para hacerlos caer en un engaño, que consiste en entregar una falsa tarjeta de Apoyo por COVID-19 a cambio de un depósito de 300 pesos que deben realizar en una tienda OXXO”, acusó.

Ante esta denuncia de fraude, la UIF investigó los movimientos financieros de la persona que como titular de la cuenta bancaria donde se depositaba el dinero que pedían a las familias que solicitaban el apoyo social.

“Al detectar la cuenta y los movimientos financieros inusuales de la persona, se procedió a congelar la cuenta y dar vista a las instituciones financieras”, indicó la UIF.

protiviti®
Face the Future with Confidence

# Cifras millonarias, por fraudes relacionados con Covid-19.

Las pérdidas por fraudes que se cometen bajo el pretexto de la contingencia que se vive en la actualidad por el coronavirus (Covid-19) comienzan a ser millonarias, y cada vez se dan con más frecuencia en distintas partes del mundo.

**07 mayo 2020**

**El Economista.**

De acuerdo con el conteo del portal econsumer.gov, el cual es administrado por la Red Internacional de Protección al Consumidor y Aplicación de la Ley (ICPEN, por su sigla en inglés), del 1 de enero al 5 de mayo de este año, se han documentado 859 reportes de distintos países de fraudes con el pretexto de la contingencia, lo cual ha resultado en pérdidas por 3 millones 600,000 dólares.

"Con denuncias provenientes de Estados Unidos, Francia, Australia, España y Chile, un aumento preocupante de fraudes refleja una explotación de los temores del público", se destaca en la página de la red que representa a más de 35 organismos internacionales de protección a los consumidores.

Según el portal donde se lleva el conteo de las quejas por fraude, la mayor parte de los engaños se basa en la venta en sitios web de tratamientos no probados, o artículos de protección como mascarillas y guantes, los cuales no son entregados. Los defraudadores se hacen pasar por agencias gubernamentales con promesas de pagos de ayuda, con la finalidad de robar el dinero de sus víctimas.

"En sitios web se venden tratamientos no probados, promoviendo pero no entregando artículos de protección como mascarillas y guantes, y haciéndose pasar por agencias gubernamentales con promesas de pagos de ayuda, pero engañando a los consumidores para que den su información personal. Y cada día surgen nuevos fraudes", explica la ICPEN.

Las cifras de este organismo reportan que las estafas comúnmente se dan por medio de servicios de comercio en línea, venta de paquetes vacacionales e inversiones, entre otros. Asimismo, las quejas que ha documentado el portal provienen principalmente de Estados Unidos, Francia, Australia, Canadá, Reino Unido y Chile.

La ICPEN destaca que los delincuentes también buscan hacerse pasar por organizaciones sin fines de lucro para recibir donaciones de gente que, de buena fe, intenta ayudar durante esta pandemia.

"Se debe investigar cuando se trata de donaciones, ya sea a través de organizaciones benéficas en su país o en el extranjero, o por sitios de crowdfunding. Algunos estafadores usan nombres que suenan como los de organizaciones benéficas reales (...) pero no lo son", acota dicha asociación.

El organismo detalla que, en este contexto, los estafadores buscan persuadir a las personas con la finalidad de convencerlas para que vendan productos para prevenir o curar el coronavirus. "Actualmente no existen ni vacunas ni tratamientos aprobados (contra el Covid-19)".

protiviti®
Face the Future with Confidence

# Cifras millonarias, por fraudes relacionados con Covid-19. (Continuación)

**07 mayo**

**2020**

El Economista.

### En Estados Unidos se agrava

Estas cifras globales son inferiores a las que arroja el gobierno de Estados Unidos. De acuerdo con la Comisión Federal de Comercio de aquel país (FTC, por su sigla en inglés), tan sólo en dicha nación, de enero al 5 de mayo de este año, se han documentado 36,238 reportes de estafas, mismas que han significado la pérdida de 24.4 millones de dólares, con una pérdida promedio de 503 dólares por estafa.

En Estados Unidos, el estado que más ha reportado fraudes con el pretexto del coronavirus es California, con 1,905 reportes, seguido de Florida, con 1,278 quejas, y Massachusetts, con 1,148 reportes.

Asimismo, el servicio por el cual se dan más fraudes de este estilo es el de la venta de viajes o paquetes vacacionales, seguido del comercio en línea, mensajes de texto y atención médica, entre otros.

protiviti®
Face the Future with Confidence

# Por Covid-19, se ha hecho mal uso del sector financiero formal: GAFI

**10 mayo**

**2020**

**El Economista.**

La emergencia sanitaria ha generado que los delincuentes intenten obtener ganancias de sus ilícitos mediante el uso del sistema financiero formal o por transacciones relacionadas con activos virtuales, según el Grupo de Acción Financiera Internacional (GAFI), organismo multilateral que genera los estándares para prevenir, detectar y combatir el lavado de dinero y financiamiento al terrorismo de forma global.

De acuerdo con Kristen Alma, analista de la secretaría del GAFI, pese a que todavía es temprano para deducir que ante la emergencia algunas tipologías de lavado de dinero se han incrementado sustancialmente, sí ha habido casos recientes donde ilícitamente se obtienen recursos que posteriormente buscan ser blanqueados por medio del sistema financiero formal, como por ejemplo en delitos como estafas en la venta de medicamentos o equipo médico.

“Es bastante temprano para identificar las tendencias (en aumento) de tipologías de lavado de dinero, pero estamos viendo un mal uso de activos virtuales y en el sector bancario formal”, explicó Alma en una conferencia en línea.

Apuntó que el organismo ha identificado tipologías relacionadas con el lavado de dinero debido a la información que ha recibido de los países miembros, entre ellos México. En este contexto, la especialista mencionó que se han detectado casos donde se piden pagos anticipados por equipo de protección médica o medicamentos, pero son una estafa.

“Ha habido un mal uso del sector bancario formal, hemos visto algunos casos de intentos de lavado de dinero relacionados con negocios que son estafas, por ejemplo, el fraude del pago anticipado para tratar de vender equipo médico de protección personal o medicamentos”, detalló Alma.

**Preocupan activos virtuales**

Dentro de la información que recibieron los analistas del GAFI, respecto a los riesgos y delitos que han surgido a partir de la pandemia del Covid-19, hay casos del mal uso de activos virtuales.

Por ejemplo, el Departamento de Justicia de Estados Unidos informó sobre el caso de un hombre, que fue detenido en aquel país por cargos relacionados con la distribución ilegal de medicamentos a través del mercado negro en Internet.

“Supuestamente (el detenido) lavó los ingresos de su actividad criminal, al cobrar en criptomonedas (Bitcoin) y los recursos los pasó a dólares estadounidenses, para trasladar los fondos a través de una variedad de cuentas, incluidas sus cuentas bancarias comerciales, en un esfuerzo por ocultar y disfrazar la naturaleza y la fuente de sus ingresos ilícitos”.

En este contexto, el GAFI indicó que ante un mayor uso indebido de servicios financieros en línea, los activos virtuales pueden ser utilizados para mover y ocultar fondos ilícitos.

La analista resaltó que la recesión económica mundial pone en el escenario el aumento de préstamos informales proporcionados por los grupos criminales, lo que es un riesgo para que dichos recursos sean lavados en el sistema financiero formal.

protiviti®
Face the Future with Confidence

# Autoridad Bancaria Europea quiere reforzar la lucha contra los fraudes de dividendos.

La Autoridad Bancaria Europea (ABE) publicó este martes un plan de acción para luchar contra los fraudes fiscales ligados a los dividendos y sacó a relucir la falta de coordinación entre los Estados miembros y las diferentes autoridades a nivel nacional.

**12 mayo**

**2020**

**El Economista.**

Casi dos años después de que estallara el escándalo "cum ex", la Autoridad Bancaria Europea publicó su informe, después de que el Parlamento Europeo la interpelara a tal efecto a finales de noviembre de 2018.

Según un consorcio de 19 medios europeos que reveló el caso en octubre de 2018, esos montajes fraudulentos o litigiosos, elaborados en Alemania, donde fueron descubiertos desde 2012, costó unos 55,000 millones de euros al fisco de once países europeos desde 2011.

El grueso de la factura, unos 46,000 millones de euros, está vinculado a una práctica de optimización llamada "cum cum". Esta técnica de arbitraje de dividendos, que según el grupo de medios estaría en "el límite de la legalidad", saca partido de la fiscalidad diferenciada entre inversores nacionales y extranjeros.

Otra práctica, llamada "cum ex", considerada fraudulenta, consiste en comprar y vender acciones en torno al día del pago de dividendos, y tan rápidamente que la administración fiscal no identifica ya al verdadero propietario.

La manipulación, que requiere la complicidad de varios inversores, permite reivindicar varias veces la devolución del mismo impuesto sobre los dividendos, perjudicando así al fisco.

Al término de su investigación, la ABE concluyó que existen diferentes apreciaciones entre las autoridades nacionales europeas sobre esos "sistemas de arbitraje de dividendos" a causa de las "diferencias entre los regímenes fiscales nacionales de los Estados miembros".

"Los sistemas de arbitraje de dividendos no son posibles en algunas jurisdicciones y, cuando lo son, no siempre son tratados como delitos fiscales", señaló la ABE, que indicó que esos montajes "atentan contra la integridad del sistema financiero" de la Unión Europea.

Encargada desde principios de 2020 de coordinar las políticas financieras europeas de lucha contra el blanqueo de dinero y la financiación del terrorismo, la ABE pretende reforzar su acción en materia de fraude de dividendos con una hoja de ruta detallada en diez puntos.

Uno de los objetivos es hacer que las autoridades nacionales y los establecimientos de crédito adopten "una visión global de los riesgos" que comportan esas técnicas de arbitraje, a través de controles y dispositivos de gobernanza internos en los establecimientos financieros.

El organismo también pidió mejoras en "el intercambio de informaciones entre las autoridades prudenciales y de lucha contra el blanqueo de dinero" y con las autoridades fiscales dentro de los Estados miembros.

La autoridad bancaria indicó asimismo que "llevará a cabo una segunda investigación formal sobre las medidas tomadas por las instituciones financieras y las autoridades nacionales para supervisar que se respetan" las nuevas exigencias.

protiviti®
Face the Future with Confidence

# Ciberdelitos aumentan en la contingencia; incrementaron 14% entre marzo y abril.

Los ciberdelitos como el fraude y la comercialización de pornografía infantil, así como la información falsa en internet, se incrementaron en un 14% entre marzo y abril, periodo de la contingencia sanitaria y confinamiento social para evitar la propagación del nuevo coronavirus (Covid-19), reveló la Guardia Nacional.

**13 mayo**

**2020**

**El Economista.**

Al participar en la mesa virtual de análisis denominada "Efectos secundarios de la crisis por el Covid-19: cibercrimen", organizada por Causa en Común, el titular de la Dirección General Científica de la Guardia Nacional, precisó que entre diciembre del 2019 y febrero del 2020 se presentó un decrecimiento del 12% en los ciberdelitos, respecto al promedio anualizado. Sin embargo, indicó que entre marzo y el 15 de abril de este año se registró un incremento del 14 por ciento.

"La situación de la pandemia sobre Covid-19 ha generado que la ciberdelincuencia dedique más tiempo a la actividad criminal mediante el uso de las tecnologías", admitió.

Destacó que las principales amenazas para los ciudadanos a través de internet es que sean víctimas de robo de información, suplantación de identidad, infección de equipos por código malicioso, acceso lógico no autorizado, fraudes cibernéticos y seguridad de la información.

Indicó que las modalidades de ello son: el phishing, donde se ofrecen supuestos programas sociales, se piden donativos o se dan prórrogas de pagos.

El segundo el smishing, mediante el cual se engaña a los usuarios con servicios gratuitos, recargas y suscripciones a plataformas de entretenimiento.

El tercero es el fraude cibernético, donde se ofrecen propiedades o vehículos a un costo por debajo del comercial.

La cuarta modalidad es el malware, o la difusión de spam; y la quinta, son las noticias falsas sobre situaciones como la contingencia del coronavirus.

Además de ello se ha descubierto el "zoombombing", que es una forma de acoso cibernético denunciado por algunos usuarios de la aplicación Zoom.

Radamés Hernández recordó que la autoridad ya detectó ligas de internet en las que se ofrecen supuestos créditos a la palabra del gobierno federal, o entrega de tarjetas del Bienestar a cambio de depositar 300 pesos en tiendas de conveniencia.

Precisó que la Guardia Nacional también detectó un vínculo, con logotipos de la Secretaría de Hacienda y de Banobras, donde supuestamente se venden vehículos de lujo a un costo por debajo del comercial.

Respecto al tema de pornografía infantil, el Dirección General Científica de la Guardia Nacional, indicó que tuvo un aumento del 73% de marzo a abril, y el 80% de los reportes están relacionados con la red social Facebook, utilizada para transmitir actividades relacionadas con la distribución de material de abuso sexual infantil.

# Ciberdelitos aumentan en la contingencia; incrementaron 14% entre marzo y abril. (Continuación)

**13 mayo**

**2020**

**El Economista.**

Por ello, para protegerse de estos ciberdelitos, llamó a los ciudadanos a tomar medidas de prevención como tener una conexión segura a internet y cambiar constantemente su contraseña, actualizar las herramientas antivirus, y utilizar cifrado de documentos al enviar mediante correos o compartir mediante dispositivos.

Puso a disposición de la ciudadanía el número 088 de la Guardia Nacional para denunciar cualquier situación de riesgo en internet, así como las direcciones @Guardia.nacional.mx en Twitter y GN_México_ en Facebook e Instagram, así como los correos: cert-mx@sspc.gob.mx; phishing@sspc.gob,mx; y malware@sspc.gob.mx.

Por su parte, Marco Antonio del Toral Morales, abogado analista del área lavado de dinero de la Oficina de Naciones Unidas contra la Droga y el Delito, dijo que "los ciberdelincuentes se aprovechan cada vez más del temor de las personas al Covid-19, y ofrecen medicamentos falsos como desinfectantes de manos y equipo médicos de protección personal inexistente, medicamentos o productos de higiene".

Alertó que el éxito de la ciberdelincuencia en el contexto actual del Covid-19, depende de los ataques de phishing por correo electrónico como fase inicial de la infección.

"Cuando la gente hace clic en un enlace o un documento, la cuenta se ve comprometida. El compromiso puede ser visible para la víctima, pero también es encubierto y permite al criminal establecer y mantener el acceso a largo plazo a la cuenta, la organización y la IP asociados", alertó.

Destacó que los ciberdelincuentes crean sitios de internet falsos para atraer a las víctimas a abrir archivos adjuntos maliciosos o hacer clics sobre los enlaces phishing.

Indicó que casi un millón de mensajes de spam se han enviado, vinculados al Covid-19, desde enero de este año. Recordó que en abril pasado, el INEGI publicó el Módulo sobre ciberacoso, donde destacó que 17.7 millones de personas fueron víctimas de ello.

La presidenta de Causa en Común, consideró que los delincuentes están aprovechando este periodo de confinamiento social para recolección de datos en internet, información confidencial y comercialización de pornografía infantil.

Mencionó que el gobierno tiene que crear una comunicación más intensa con la ciudadanía para que pueda estar enterada de las nuevas modalidades de delitos de los que puede ser víctima a través de internet.

Finalmente, el presidente y Fundador de MaTTica, consideró que se requiere actualizar el marco jurídico para sancionar de mejor manera los ciberdelitos. Apuntó que no se requieren grandes reformas, sino únicamente actualizar temas relacionadas con acceso a la información y fraudes.