Boletín de Fraude 30 de Abril 2020

01 Extorsión, segundo delito más recurrente en México.

02 Delincuentes ven actual situación propicia para disfrazar dinero ilícito.

03 Ciberfraudes, delitos por internet y otros riesgos ante aislamiento por COVID-19.

04 Riesgos en tiempos de Covid-19.

05 Fabricante de las N95 lanza página y línea para denunciar fraudes y altos precios.

06 Ciberataques en contingencia buscan más a usuarios financieros: expertos.

¿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

Extorsión, segundo delito más recurrente en México

16 abril

2020

El Economista.

De enero 2019 a febrero 2020, alrededor de 111,0000 mexicanos denunciaron algún tipo de extorsión al número telefónico 089, convirtiéndose así en el segundo delito del fuero local más recurrente en el país, después del robo o asalto en la calle o transporte público. De acuerdo con un documento del Centro Nacional de Información (CNI), obtenido por El Economista, uno de cada cinco delitos cometidos en 2018 fue una extorsión.

Se estima que en el 2018 se cometieron 5.7 millones de extorsiones, el 91.6%. Las autoridades del CNI y de la Secretaría de Seguridad y Protección Ciudadana (SSPC) tienen datos de que entre 2017 y 2018 se observó un incremento significativo en las extorsiones concretadas; es decir, que el ciudadano afectado pagó lo solicitado. “Derivado del aumento en la efectividad de las extorsiones, el monto económico recaudado por el crimen alcanzó un máximo histórico (12,000 millones de pesos)”, cantidad que es equivalente a lo destinado por el gobierno federal este año a los estados en dos fondos de seguridad: FASP y FORTASEG.

Según el documento del CNI, la extorsión es el delito más frecuente en 14 entidades federativas: Sinaloa, Durango, Zacatecas, San Lui Potosí, Tamaulipas, Hidalgo, Veracruz, Guerrero, Michoacán, Jalisco, Nayarit, Morelos, Tlaxcala y Colima.

Se menciona que en el 2018, el delito de robo o asalto en la calle o transporte público ocupó el primer lugar de los delitos del fuero local con 29%; seguido de la extorsión con 17%; el fraude con 14%; el robo de vehículo con 12%; las amenazas 9%; el robo a casa habitación con 7%; entre otros delitos. En el periodo de enero 2019 a febrero 2020, casi 111,000 mexicanos denunciaron una extorsión al 089”, refirió.

El CNI estima que para revertir la tendencia se requiere de una campaña de comunicación para hacerle saber a los ciudadanos que ya es seguro denunciar los números de extorsión o fraude al 089, así como coordinar acciones de investigación e inteligencia con la Guardia Nacional, la Unidad de Inteligencia Financiera y Fiscalías Estatales.

El gobierno federal a través de la SSPC y el CNI se proponen crear una base de datos de los números telefónicos origen de la extorsión, a fin de recabar la información útil sobre las formas que la población reporta al número nacional de denuncia anónima 089. También se propone establecer protocolos de intercambio de información entre las diversas instancias de seguridad para el combate frontal de este delito, y coadyuvar con el proyecto de Ley para el Registro Nacional de Números Telefónicos, “lo que permitirá mitigar las extorsiones o fraudes”. La base de datos incluirá el número telefónico del presunto extorsionador; tipo de extorsión o fraude; entidad y municipio de la víctima; fecha y hora de la extorsión; sexo y edad aproximada de las partes; modus operandi; los bienes entregados en su caso en dinero o en especie, entre otros.

Y es que el gobierno federal reconoce que a la fecha, existen pocos esfuerzos para prevenir las extorsiones y fraudes; los datos que hay sobre el delito son insuficientes y la gente no sabe qué hacer si es víctima de una extorsión.

Paseo de la Reforma 243 Piso 18 Suite 16 Col. Cuauhtémoc 06500 México D.F. Conmutador 6729- 8070 Fax: 5511.2500

protiviti®
Face the Future with Confidence

Delincuentes ven actual situación propicia para disfrazar dinero ilícito.

19 abril

2020

El Universal.

La compleja situación económica que atraviesan países como México, debido a la contingencia del coronavirus (Covid-19), es una gran oportunidad para que la delincuencia busque lavar sus recursos ilícitos mediante el sistema financiero, por lo que las entidades financieras deben estar alertas para mitigar los riesgos que se deriven de esta pandemia, precisa un documento de la Comisión Nacional Bancaria y de Valores (CNBV).

Recientemente, el órgano regulador emitió su guía sobre los riesgos de lavado de dinero y financiamiento al terrorismo con el fin de que los integrantes del sistema financiero identifiquen y combatan desafíos, amenazas y vulnerabilidades derivadas de la contingencia sanitaria del Covid-19.

“Se espera que los sujetos supervisados implementen dicho documento a fin de prevenir y detectar los actos, omisiones u operaciones (de lavado de dinero o financiamiento al terrorismo)”, se lee en el documento, el cual se distribuye a integrantes del sistema financiero y del cual este medio tiene una copia.

Ahí se destacan seis conductas que pueden detonar el lavado de dinero o el fortalecimiento de las estructuras financieras terroristas, derivadas por la contingencia del Covid-19 y éstas son: fraude, delitos informáticos, cambios en el comportamiento financiero de una persona, corrupción, aprovechamiento de la volatilidad del sistema financiero y financiamiento al terrorismo.

Respecto al fraude, en línea con diversos organismos, la CNBV indica que la contingencia puede ser aprovechada por la delincuencia para obtener recursos mediante estafas tales como la venta de medicamentos o pruebas falsas para detectar el Covid-19 y, además, los estafadores pueden identificarse como servidores públicos para robar datos personales de sus víctimas con el fin de realizar operaciones a nombre de ellas.

La CNBV señala que los delincuentes pueden aprovecharse del uso del Internet para cometer delitos informáticos, como la utilización de códigos maliciosos para asumir el control de computadoras o dispositivos, con el objeto de obtener recursos de sus víctimas.

Medios electrónicos

La CNBV precisa que el potencial aumento en el uso de medios electrónicos también representa un riesgo, pues puede haber operaciones que no tengan una explicación razonable respecto a los montos, origen o destino de los recursos, o que se realicen por medio de la banca en línea y, sin razón aparente, se cambien datos de los clientes.

Además, refiere que puede haber riesgo por operaciones realizadas por personas vulnerables a sufrir fraudes financieros, debido a su poco o nulo conocimiento de la banca electrónica.

Enfatiza que también se pueden generar operaciones de actos de corrupción a partir de la contingencia, por ejemplo, la apropiación indebida de recursos públicos derivada de procesos de adquisiciones y contratos gubernamentales o el desvío o transferencias de fondos a otros países.

BOLETIN DE FRAUDE.

protiviti®
Face the Future with Confidence

Ciber fraudes, delitos por internet y otros riesgos ante aislamiento por COVID-19.

El jefe de la Unidad de Inteligencia Financiera, Santiago Nieto Castillo, reconoció este viernes que en el marco de la contingencia sanitaria por el COVID-19, la delincuencia "al final del día no se detiene, se está moviendo a otros elementos".

24 abril

2020

El Financiero.

En reunión virtual con legisladores de la Comisión de Hacienda y Crédito Público de la Cámara de Diputados, alertó del crecimiento de fraudes y delitos como la venta de pruebas falsas del COVID-19, medicamentos apócrifos, y en la contratación de servicios por internet.

También hizo énfasis en los fraudes por internet y redes sociales, el uso de transmisores de dinero y la utilización de depósitos en cuentas del sistema financiero que son retiradas de manera inmediata.

Por ello dijo que el objetivo es generar políticas públicas que atiendan esto, afirmó.

Santiago Nieto precisó que con el cierre de las empresas no esenciales se ha incrementado el uso del trabajo remoto y la interacción social en línea, por lo que "ese es el primer tema que tenemos que ver como riesgo, en virtud de que la actividad de la delincuencia organizada va a brincar de la ordinaria a la de línea, lo cual tiene un efecto importante en temas de defraudación".

Nieto dijo que se requieren mecanismos que permitan fortalecer la economía en el ámbito de lo formal, pues cuando se tiene este tipo de pandemias, uno de los impactos directos es que el dinero empieza a circular en efectivo y en ámbitos fuera de la economía formal.

Esto "genera un riesgo porque se tiene más efectivo circulando y esto provoca posibles casos de corrupción y temas relacionados con delincuencia organizada".

Mencionó que a consecuencia de la pandemia COVID-19, en el ámbito mundial ha habido un aumento de fraudes financieros por impostores vía internet, suplantación o por venta de productos o inversiones que no existen. También, adulteración o falsificación de medicamentos, así como venta de pruebas falsas, "de esto último ya se han conocido casos en México".

Nieto añadió que se debe plantear las posibilidades de que se reciban mensajes para usurpar identidades: "debemos estar pendientes de que no se usen cuentas falsas que pidan dinero y que eso también pase con empresas farmacéuticas que empiecen a ser falsificadas en su mecanismo de operación".

El funcionario expuso que se ha duplicado la venta de insumos que no cumplen con los criterios específicos que necesita el sector salud, como son mascarillas o gel antibacterial.

En el tema de la corrupción política en este tipo de casos, dijo, se da en las contrataciones gubernamentales y "aquí el proceso ha sido acompañar a las instancias para evitar que se presenten actos de corrupción, pero debemos tener presente que hay un aumento en las operaciones sustanciales en términos financieros y que son de carácter remota y no presenciales, lo que provoca nuevos riesgos para las personas que generan actividad comercial".

protiviti®
Face the Future with Confidence

Ciber fraudes, delitos por internet y otros riesgos ante aislamiento por COVID-19. (Continuación)

Otro tópico a cuidar, abundó, tiene que ver con el incremento de las casas de empeño, prestamistas y medios de financiamiento informal. “El riesgo es que se eleve el número de empeños respecto a la práctica cotidiana que se tiene en el país”.

24 abril

2020

El Financiero.

El desempleo, dijo, también puede generar un aumento de reclutamiento de personas por parte de la delincuencia organizada, “es algo que hay que tener con claridad. Por lo tanto, soy partidario de que los programas sociales del Gobierno Federal se estén manteniendo y haya apoyos para las micro, pequeñas y medianas empresas, para poder generar un mecanismo de protección”.

Se debe revisar a las organizaciones sin fines de lucro, porque en muchas ocasiones se pueden ver dos elementos negativos: que sean verdaderas pero que se esté haciendo un mal uso de ellas para lavar dinero en estos momentos de contingencia, y por otro lado, el surgimiento de organizaciones sin fines de lucro falsas, que empiezan a recopilar dinero por internet o redes sociales.

“Nosotros estamos en este proceso de revisar que no nos encontremos en presencia de este problema de mal uso de las organizaciones sin fines de lucro, pero sobre todo que no se generen otras falsas para estar defraudando a la sociedad mexicana”, expuso.

Reconoció que la corrupción, por supuesto, existe aun cuando hay pandemia. Tan sólo el IMSS, agregó, ha denunciado un caso de robo en almacenes. “Lo importante es evitar el desvío de los fondos y bienes que se tienen para enfrentar la contingencia y también evitar que ese dinero sea mal utilizado y evitar otra “Estafa Maestra” u otros procesos en donde aparecen empresas fachada que terminaban ganando las contrataciones. Es algo que tenemos que evitar en este momento”.

Sobre los menores y el uso de internet, afirmó que ahora se corre un mayor riesgo porque tienen mayor presencia en internet y redes sociales, y están expuestos a temas de pornografía infantil, explotación y trata de personas.

De igual modo, pidió estar atentos a lo que pasa en las aduanas, en lo particular, con el fentanilo. Se debe asegurar que llegue a las farmacéuticas y hospitales, y así evitar que pueda ser trasladado a otros lugares para producir los psicotrópicos que terminan privando de la vida a las personas. “Hay un problema real en aduanas y es algo que se tiene que atacar”.

protiviti®
Face the Future with Confidence

Riesgos en tiempos de Covid-19.

26 abril

2020

El Economista.

Estimado lector, es frecuente que, durante diversos episodios de desastres naturales, de pandemias y de crisis económicas se den casos, con diverso grado de intensidad, de desvío de recursos públicos destinados a atender tanto la emergencia, como la recuperación. Estos problemas se dan en diversas latitudes.

La consecuencia inmediata de los actos de corrupción en general es la pérdida de eficacia en las acciones del Estado, lo cual afecta a la población e incide en la pérdida de confianza.

La OECD discute en un documento reciente (abril de 2020) estos problemas: "Public Integrity for an Effective Covid-19 Response and Recovery", en el que llama la atención sobre casos de desastres naturales, pandemia y crisis económicas en las cuales se crearon oportunidades de fraude y riesgos de corrupción al relajarse las políticas de integridad en los procesos de compra, en los paquetes de estímulos económicos y sociales, y en la asignación de obra pública, entre otros.

Crisis de desastres naturales y pandemias como el Huracán Katrina (2005) y el Ébola (2014-2016) muestran que la adopción de procedimientos especiales de compra y de asignación de recursos públicos pueden ser solventados a expensas de los ciudadanos. También es el caso de los recursos canalizados para la recuperación económica (2008-2009) a la Unión Europea en que se detectaron riesgos de corrupción, fraude, desperdicio y abuso. La OECD concluye que, "en ausencia de salvaguardas de integridad y transparencia los procedimientos de emergencia son vulnerables al abuso".

La crisis del Covid-19 ha obligado a los estados nacionales y sub-nacionales a tomar medidas sobre la marcha, muchas veces extremas, para contrarrestar las oportunidades de fraude y corrupción. Estas medidas han consistido en: revisar y reforzar los procedimientos de adquisiciones emergentes; establecer y fortalecer mecanismos justos, equitativos y transparentes de contratación; llevar a cabo políticas públicas de exención a la emergencia bajo el criterio de "libro abierto" al escrutinio público; establecer procedimientos reforzados de control interno que verifiquen en tiempo real adquisiciones, contrataciones y distribución de bienes y servicios.

Entre los países que se distinguen por haber asumido medidas extraordinarias de control y transparencia ante la crisis se encuentran Irlanda, el Reino Unido y Japón.

La buena gobernanza y el control interno son fundamentales porque mitigan los riesgos de fraude con medidas de compliance o de cumplimiento normativo. La Guía 5270 de la Organización Internacional de Entidades Fiscalizadoras Superiores (INTOSAI, por sus siglas en inglés) señala que la promoción de la gobernanza es necesaria para evitar distorsiones en las decisiones de política pública.

La trazabilidad del gasto público es una pieza clave para blindar el uso y el destino de los recursos asignados de manera emergente. Además de la documentación estricta, los procesos de compra, debe ponerse énfasis en la reprogramación, ejecución y control del gasto. Como queda evidenciado, incluso en tiempos de emergencia, es fundamental el apego y el respeto a los valores del Buen Gobierno y la Democracia.

BOLETIN DE FRAUDE.

protiviti®
Face the Future with Confidence

Fabricante de las N95 lanza página y línea para denunciar fraudes y altos precios.

La empresa fabricantes de cubrebocas N95 y otros productos de protección personal ante la pandemia del nuevo coronavirus, lanzó un sitio de internet y una línea telefónica para reportar actividades fraudulentas y el aumento de precios.

27 abril

2020

El Economista.

“Desde el inicio de la pandemia, la empresa ha identificado y atendido alertas y denuncias sobre personas que se presentan fraudulentamente como distribuidores o vendedores de productos de la compañía, ofreciendo productos falsificados o que falsamente afirman fabricar nuestros productos , indicó la empresa en un comunicado”.

Agregan que los precios de los cubrebocas N95 de la empresa se han mantenido igual que antes de la pandemia, aunque no pueden controlar los precios que cobran los distribuidores, por lo que han exhortado a toda la cadena de distribución a hacer lo mismo.

“La empresa también está trabajando con importantes operadores de comercio electrónico y redes sociales en un plan coordinado para identificar y eliminar a falsificadores y vendedores poco éticos de sus sitios web. Los equipos de la empresa monitorean e informan todos los días sobre sitios web o páginas de redes sociales fraudulentas, para evitar confundir al público”, refirió la empresa.

Ciberataques en contingencia buscan más a usuarios financieros: expertos.

El mayor uso de servicios financieros digitales que se ha detonado a partir de la emergencia mundial por el coronavirus (Covid-19) también ha provocado un incremento en el número de ciberataques, los cuales, en el contexto actual, están más enfocados a los usuarios que a las instituciones, indicó analista senior de firma de ciberseguridad.

28 marzo

2020

El Financiero.

En entrevista, el analista indicó que la contingencia que se vive actualmente ha develado que los ciberataques son de mayor sofisticación que antes, con el fin de sustraer información de los usuarios financieros que apuestan por el uso de herramientas digitales para llevar a cabo sus operaciones.

“En esta circunstancia actual de contingencia, lo más común son ataques hacia los usuarios, claro, sin descartar que puede haber ataques a sistemas financieros en todo el mundo, pero actualmente puede resultar más atractivo el ataque a los usuarios”, detalló el experto en ciberseguridad.

Analista de ciberseguridad reconoció que todavía hace algunos años, este tipo de ataque a los usuarios de servicios financieros era más fácil de detectar, pues las herramientas por las cuales pretendían robar información tenían errores graves, como faltas de ortografía, una redacción incoherente, entre otros.

“Normalmente, este tipo de actividades era más fácil de detectar porque te consumía una cantidad importante de recursos. hoy en día, están perfeccionadas y es difícil detectarlas”, señaló.

El experto menciona que la metodología más común que se ha observado actualmente es el de la ingeniería social, donde por medio de mensajes, correos electrónicos o llamadas telefónicas, se busca obtener información financiera de las personas para hacer mal uso de ella.

El experto en ciberseguridad recomendó que, si una persona busca utilizar servicios financieros en línea, tenga en cuenta el riesgo al que está expuesto y utilice herramientas que ayuden a detectar cualquier irregularidad que pueda poner en peligro su información.