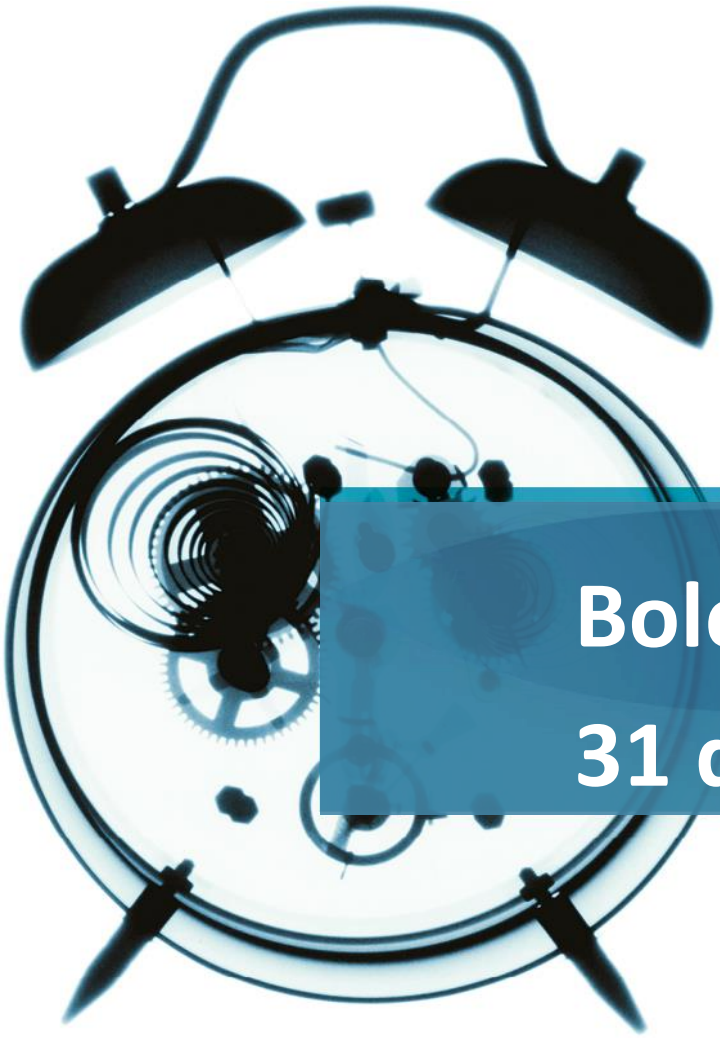

protiviti®
Face the Future with Confidence

Boletín de Fraude
31 de Enero 2020

Protiviti líder en servicios de consultoría de riesgos de negocios y auditoría interna, apoya a la lucha antifraude.

Quincenalmente distribuimos esta recopilación de las noticias más sobresalientes relacionadas con delitos de cuello blanco.

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

CONTÁCTANOS

16 de enero

Por posible robo de identidad, clientes de la banca pierden 2 mil 965 mdp: Condusef.

20 de enero

Nueva estafa podría robar tu cuenta de WhatsApp.

21 de enero

Compañía de reconocimiento facial acabará con tu privacidad.

26 de enero

Quejas por fraudes cibernéticos aumentaron 38% en el 3T del 2019: Condusef

27 de enero

Se disparan ciberataques contra bancos; cuestan 784 mdp.

27 de enero

Fintech apuestan por la tecnología; buscan optimizar su sistema.

BOLETÍN
Enero 2020

16 de enero

El Universal.

Por posible robo de identidad, clientes de la banca pierden 2 mil 965mdp: Condusef.

De enero a septiembre de 2019, usuarios del servicio financiero en México perdieron 2 mil 965 millones de pesos, por posible robo de identidad, con un total de 55 mil 102 reclamaciones, lo que representa un incremento de 10.5% respecto del mismo periodo del año previo, informó la Comisión Nacional para la Protección y Defensa de los Servicios Financieros (Condusef).

Según los datos del organismo, del monto reclamado por los usuarios, les fueron abonados mil 151 millones de pesos, equivalente a 41% del total donde 4 de cada 10 casos se resolvieron a favor del usuario afectado.

La Condusef resaltó que, en el caso de posible robo de identidad cibernético, se presentó un aumento de 160% en el periodo de referencia, con un total de 5 mil 418 casos.

En marzo próximo, los bancos que operan en México deberán aplicar por ley controles biométricos, principalmente lectores de huellas dactilares para cotejar la información de los clientes con la base de datos del Instituto Nacional Electoral, con el objetivo de disminuir los casos de robo de identidad en el país.

Se disparan quejas contra servicios financieros.

En la información de la Condusef se muestra de enero a septiembre de 2019, las quejas totales contra los servicios financieros en México crecieron 23.3%, con un total de 6 millones 614 mil reclamaciones.

Dicha cifra representó un monto total reclamado por parte de los clientes de 16 mil 774 millones de pesos, de los cuales solamente se abonaron 6 mil 593 millones de pesos a los usuarios afectados.

La Condusef resaltó que, en el periodo de referencia, los fraudes cibernéticos crecieron 38%, con un total de 4 millones 359 mil quejas, equivalente a 66% del total.

En este caso, los clientes afectados reclamaron un total de 8 mil 568 millones de pesos, de los cuales solamente se les devolvió 43% y 8 de cada 10 casos se resolvieron en favor de los afectados.

20 de enero

El Universal.

Nueva estafa podría robar tu cuenta de WhatsApp.

Dada la popularidad de WhatsApp la aplicación de mensajería está en la mira de los ciberdelincuentes que quieren aprovecharse de los usuarios y robar sus cuentas para cometer fraudes.

La última estafa, reportada por una compañía de seguridad cibernética, consiste en una llamada en la que un supuesto organizador de eventos afirma al usuario que ganó entradas gratis a una función o concierto.

El estafador dice que envió un código SMS a la víctima y pide que le comparta los seis números recibidos para confirmar los boletos.

La realidad es que no ganó ningún premio, se trata de una táctica destinada a robar cuentas de WhatsApp que se ha vuelto muy popular en los últimos meses y es que, lo que la víctima no sabe es que en realidad esos seis números que entrega son los códigos de verificación de su cuenta de WhatsApp.

Al compartir dicho código el criminal puede y tomará control de la cuenta de la víctima dándole acceso a toda la información, contactos, imágenes y conversaciones disponibles ahí. Al parecer la intención del criminal es hacerse pasar por la víctima y pedir dinero a sus contactos. También es posible que quiera utilizar la información que encuentre para chantajear a la víctima.

Una vez que logran engañar al usuario los delincuentes habilitan la autenticación de doble factor en las cuentas que no contaban con esta función, lo que impide que el verdadero propietario recupere su cuenta, de ahí la importancia de activar esta configuración. “La autenticación de doble factor siempre ha sido la única forma de evitar el robo de las cuentas de WhatsApp, pero ahora los malhechores la están usando para mantener a los dueños reales sin acceso a sus cuentas. Esto recalca la necesidad de que las personas entiendan la importancia de proteger sus datos. Instamos a todos los usuarios a que configuren la autenticación de doble factor en esta aplicación lo antes posible y desconfíen de mensajes y llamadas de desconocidos, ya que no todo lo que brilla es oro”, advierte analista de seguridad.

21 de enero

El Universal.

Compañía de reconocimiento facial acabará con tu privacidad.

Cientos de agencias de aplicación de la ley en Estados Unidos han comenzado a utilizar un nuevo sistema de reconocimiento facial, así lo reveló una nueva investigación realizada por el diario The New Times. La base de datos está compuesta por miles de millones de imágenes extraídas de millones de sitios, incluidos Facebook, You Tube y Venmo. El rotativo señalo que el trabajo de la empresa biométrica podría "terminar con la privacidad tal como la conocemos", y vale la pena leer la pieza en su totalidad.

El uso de sistemas de reconocimiento facial por parte de la policía ya es una preocupación creciente, pero la escala de la base de datos de la empresa biométrica, sin mencionar los métodos que usó para ensamblar, el particularmente preocupante. El sistema de reconocimiento facial se basa en datos de más de tres mil millones de imágenes eliminadas de internet, un proceso que puede haber violado los términos de servicio de los sitios web. Los organismos encargados de hacer cumplir la ley pueden subir fotos de cualquier persona de internet de sus casos, y el sistema devuelve imágenes coincidentes de internet, junto con enlaces a donde se alojan estas imágenes, como los perfiles de redes sociales.

The New York Times, indicó que el Sistema ya ha ayudado a la policía a resolver crímenes que incluyen robos en tiendas, identificación de robos, fraudes con tarjetas de crédito, asesinatos y explotación sexual infantil. En un caso, la Policía del Estado de Indianápolis pudo resolver un caso en 20 minutos utilizando la aplicación.

No obstante, el uso de algoritmos de reconocimiento facial por parte de la policía conlleva riesgos. Los falsos positivos pueden incriminar a las personas equivocadas y los defensores de la privacidad temen que su uso puede ayudar a crear un estado de vigilancia policial. Según los informes, los departamentos de policía han utilizado imágenes manipuladas que podrían conducir a arrestos injustos, un estudio federal ha descubierto "evidencia empírica" de sesgo en los sistemas de reconocimiento facial.

De igual manera, la utilización del sistema implica subir fotos a los servicios del biométrico, aún no está claro, que tan seguros son. Aunque señaló que sus empleados de atención al cliente no ven las fotos que se cargan, parece ser consciente de que la periodista del Times que investiga el artículo estaba haciendo que la policía buscara su rostro como parte de su información: "Mientras la compañía me esquivaba, también me estaba monitoreando. A petición mía, varios agentes de policía pasaron mi foto a través de la aplicación. Pronto recibieron llamadas telefónicas de representantes de la compañía preguntando si estaba hablando con los medios, una señal de que la aplicación tiene la capacidad y en este caso, el apetito de controlar a quién busca la policía.

The Times informó que el sistema parece haberse vuelto viral en los departamentos de policía, con más de 600 ya registrados. Aunque no ha habido una verificación independiente de su precisión, la reportera indicó que el sistema pudo identificar fotos de ella incluso cuando cubrió la mitad de su rostro y que logró encontrar fotografías de ella que nunca había visto.

26 de enero

El Economista.

Quejas por fraudes cibernéticos aumentaron 38% en el 3T del 2019: Condusef.

El director de Educación Financiera Citibanamex, Juan Luis Ordaz, aseguró que uno de los fraudes más comunes con tarjetas de crédito es la clonación, que en el último año aumentó 38 por ciento.

El especialista explicó que el delito consiste en robar la información contenida en el plástico a través de dispositivos electrónicos, para después transferir la información a una nueva tarjeta vacía, permitiendo a los delincuentes pagar en comercios o extraer dinero de la cuenta del afectado.

De acuerdo con cifras de la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (Condusef), al tercer trimestre de 2019, las quejas por fraudes cibernéticos ascendieron a más de seis millones, crecieron 38% respecto de 2018.

Detalló que el fraude y clonación son ilícitos que cada año aumentan en mayor proporción con respecto a las estafas tradicionales, esto es 66% para fraudes cibernéticos y 34% para los tradicionales.

Juan Luis Ordaz destacó que el monto reclamado de los fraudes cibernéticos ascendió a 8,568 millones de pesos y aun cuando 86 de cada 100 fraudes cibernéticos se resolvieron a favor del usuario, es un delito que requiere de tiempo para resolverse.

Reiteró que uno de los fraudes más comunes con tarjetas de crédito es la clonación y es posible que el cliente no se dé cuenta del robo hasta que recibe el saldo del banco en cero o con cargos por consumos o servicios no realizados.

"Si eres víctima de este delito y descubres operaciones que no realizaste, tienes hasta 90 días, contados a partir de la fecha en que se realizó el cargo, para reclamar en tu banco" indicó el director de educación financiera de Citibanamex.

Sin embargo, recomienda prevenir para evitar que la tarjeta de crédito sea clonada primero en cajeros automáticos, realizar sólo las operaciones y no solicitar ayuda de personas extrañas, además de cerciorarse de que nadie conozca el Número de Identificación Personal (NIP) y cambiarlo frecuentemente.

Sugiere siempre recoger la tarjeta, dinero y comprobante impreso. Reportar de inmediato si el cajero automático retiene la tarjeta. Y en los establecimientos se debe solicitar que todos los pagos se realicen a la vista. Además de guardar comprobantes, para posibles reclamos.

Ahora que, si las operaciones son en internet, Ordaz aconsejó no realizar operaciones en redes públicas, sino desde su casa o redes seguras.

Finalmente, consideró que una herramienta de gran ayuda es el servicio de notificaciones del banco, para estar al tanto de todos los movimientos de las cuentas que se tienen.

27 de enero

El Universal.

Se disparan ciberataques contra bancos; cuestan 784 mdp.

En un año, los ataques cibernéticos contra las instituciones financieras pasaron de uno a cuatro por trimestre, lo que representó afectaciones por 784.7 millones de pesos, reveló el Reporte de Estabilidad Financiera del Banco de México (Banxico) a diciembre de 2019.

Además, hubo una diversificación en cuanto a los servicios afectados, "desde transferencias electrónicas hasta cajeros automáticos" reconoce Banxico.

Los medios de ataque fueron variados, pues se observó la vulneración de software, operaciones fraudulentas ejecutadas por terceros laborando al interior de la institución, robo de contraseñas, abuso de deficiencias en la validación de saldos y vulneración de equipos de telecomunicaciones, entre otros.

Los ataques se enforcaron en vulnerar sistemas conectados a los bancos que no fueron desarrollados por las instituciones sino por algún tercero, como los canales de banca móvil y los provistos por corresponsales o empresas Fintech asociadas como los bancos.

El documento reconoce que los ciberdelincuentes muestran amplio conocimiento de protocolos y sistemas de interconexión para acceder a cuentas y servicios de transferencia de los bancos.

Para los hackers y ciberdelincuentes atacar un banco representa un reto de inversión, señala empresa de defensa cibernética. "Desafortunadamente, las amenazas hacia las instituciones bancarias nunca desaparecerán por completo, deben existir controles efectivos para desalentar estos ataques desde un punto de vista criminal, pero cada institución necesita una estrategia de seguridad integral que evolucione con la empresa moderna y los códigos de ataque cambiantes", subrayó.

Los hackers son oportunistas y quieren maximizar sus ganancias o impacto con un trabajo mínimo. "Cuando alrededor de 300 millones de pesos fueron robados de los bancos mexicanos, éstos se convirtieron en un objetivo más atractivo para los hackers, las debilidades conocidas en el SPEI probablemente trajeron más actores cibernéticos al campo de juego".

Surgimiento criminal.

Analista de empresa de seguridad cibernética, explicó que hay un surgimiento de grupos cibercriminales locales, regionales y globales, ya que, al existir huecos legales, el costo-beneficio de estas actividades puede ser mayor que el riesgo al que se enfrentan.

Para hacer frente a estos ataques, se aconseja que el primer paso a dar por parte de las instituciones consiste en orientar sus esfuerzos de formar más estrategia, apoyándose en información de inteligencia que les permita conocer a sus adversarios, así como las técnicas, herramientas y procedimientos que utilizan para realizar sus ataques. "Esto los colocará en una mejor posición para detectar de forma temprana y responder adecuadamente a un compromiso de seguridad", manifestó.

27 de enero

El Universal.

Se disparan ciberataques contra bancos; cuestan 784 mdp. (Continuación)

Especialista de seguridad informática, agregó que otro inconveniente radica en que las regulaciones no se cumplen por completo, a pesar de que tiene el carácter de obligatorias, incluso algunas directrices se presentan como opcionales y por tal razón no son acatadas.

Enemigo en casa.

De las afectaciones por 784.7 millones de pesos registradas durante 2019, el incidente que representó un mayor golpe a la banca mexicana fue el de un fraude realizado por personal de terceros que trabajaban dentro de la institución bancaria.

El acto consistió en que inyectaba operaciones apócrifas de depósito de intereses a cuentas de cheques a través de un archivo para cargar por lote desde un ambiente de desarrollo. Esta acción se repite por tres días.

La afectación causada a esta institución de banca de inversión fue de 462 millones de pesos. "Los empleados tienen las claves y el conocimiento íntimo de los procesos internos, además de la ubicación de los datos".

Por los que las soluciones de seguridad deben considerar lo que entra y sale de la empresa, así como lo que sucede en el interior.

El director de seguridad informática dijo que, para detectar una amenaza interna, las instituciones financieras deben buscar herramientas de seguridad cibernética que puedan aprender patrones de comportamiento para empleados y personal de terceros.

Por su parte, advirtió que los bancos que contratan a terceros deben contemplar en sus políticas sanciones en caso de incumplimiento a las normas. "La aplicación de controles técnicos que permiten identificar anomalías es otra práctica necesaria para guardar evidencias y rastrear actividades fraudulentas".

27 de enero

Excelsior.

Fintech apuestan por la tecnología; buscan optimizar su sistema.

La inclusión de Big Data, Inteligencia Artificial, Cloud, Blockchain, Red 5G, IoT, así como innovaciones en biometría y robótica, son tendencias que estarán presentes en las Fintech durante este 2020, así lo adelanta especialista en tecnologías financieras.

"Durante este año vamos a ver cómo startups y empresas con más experiencia apostarán aún más por la inclusión tecnológica a sus servicios y soluciones, a través de integraciones de blockchain, inteligencia artificial, big data entre otros desarrollos que se encuentran actualmente en gestión", detalla.

En el estudio presentado en 2019, se precisa que las nuevas tecnologías serán fundamentales para el desarrollo de los servicios financieros, incluso se hablaba de que experimentarían una transformación total que además de beneficiar a los usuarios, marcaría un parteaguas en cómo se desarrolla esa industria.

Sobre ese punto, explican que los avances y tendencias digitales que se vislumbran desde finales de 2019 serán una gran oportunidad para las empresas financieras que deseen ofrecer nuevas ofertas y servicios o soluciones realmente personalizadas y en tiempo real.

Sin embargo, este informe detalla que, para lograr la inclusión e implementación de nuevas iniciativas, por ejemplo, con inteligencia artificial o internet de las cosas, sería necesario que los ejecutivos apuesten por esos proyectos de manera constante, y den un paso hacia adelante, pues hasta ahora menos del 40 por ciento de los líderes de empresas del sector financiero, ha avanzado en su desarrollo e implementación.

Con el despliegue de las redes 5G, el uso de dispositivos de IdC conectados aumentará rápidamente, incrementando masivamente la vulnerabilidad de las redes ante los ciberataques de 5ª generación multisectoriales y de gran escala. Los dispositivos de IdC y sus conexiones con redes y nubes siguen siendo un eslabón débil de la seguridad.

Las organizaciones ya manejan la mayoría de sus cargas de trabajo en la nube, pero todavía no se entiende bien lo que significa la seguridad en la nube. Las soluciones de seguridad en la nube han de transformarse en formas nuevas y flexibles que ofrezcan protección con rapidez.

"Hay países en donde ya es una realidad la oferta de servicios financieros tecnológicos, que cuentan con el conocimiento de blockchain o aplicación del Big Data, sin embargo, la falta educación financiera y tecnológica es uno de los aspectos que detiene el desarrollo de las fintech en ese sentido".

"En el caso de México, nos encontramos en la fase de regulación del sector Fintech, estamos avanzando hacia la operación regulada lo cual nos sigue manteniendo como líderes en la región de América Latina, por lo que podremos ver durante este año, cómo las fintech mexicanas evolucionan a una etapa avanzada de inclusión tecnológica y para lograrlo, harán uso de soluciones como el Internet de las Cosas (IoT) o la biometría que ya se aplican en otras ramas e industrias".