E-ISSN 2619-6301 No. 14, Año 2021

ANÁLISIS PRELIMINAR DE LA CIBERSEGURIDAD ASOCIADA AL SISTEMA FINANCIERO EN ALGUNOS PAÍSES DE LATINOAMÉRICA Y LA CONTRIBUCIÓN DE LA INFORMÁTICA FORENSE

Mayra A. Arévalo Álvarez*, Daniel Andrey Hernández Ladino**

RESUMEN

El sistema bancario ha expandido sus servicios fuera de la planta física, de manera que ha tomado mayor auge en la plataforma *web* y móvil. Por esta razón, se presenta la necesidad de brindar un mejor esquema de seguridad que vaya a la par con la prevención, pero también con la generación de una respuesta más eficaz ante un eventual ataque. Por medio de una investigación sobre algunos de los países de Latinoamérica, se buscó identificar si los bancos se han visto expuestos a algún tipo de amenaza en años recientes, asociada con su auge en la nube, qué medidas de prevención han tomado o han buscado implementar para contrarrestarlas y cuál es la contribución que ofrece o puede ofrecer la informática forense en el propósito de ayudar a esclarecer procesos de investigación, principalmente relacionados con delitos financieros.

Palabras clave: Amenazas, Bancos, Ciberseguridad, Delitos financieros, Evidencias, Informática forense, Latinoamérica, Metodología, Herramientas forenses

* Estudiante, Ingeniería de Sistemas, Fundación Universitaria del Área Andina. Correo electrónico: mareavalo31@estudiantes.areandina.edu.co
** Estudiante, Ingeniería de Sistemas, Fundación Universitaria del Área Andina. Correo electrónico: dhernandez142@estudiantes.areandina.edu.co

OBJETIVO

El objetivo de este artículo es investigar las amenazas más recientes a las que está expuesto el sistema bancario en algunos países de Latinoamérica, las acciones que están tomando para manejarlas y la contribución que la informática forense puede ofrecer para ayudar al esclarecimiento de delitos financieros.

Introducción

El mundo, en su realidad actual, entra a una nueva era hacia un cambio de paradigma, tanto como lo fue el surgimiento del Renacimiento o la Primera Revolución Industrial, debido a la afectación de impacto global que supuso la pandemia generada por el Covid-19. Esta situación ha llevado a que las personas centren su atención en los medios informáticos que permiten no solo mantenerse al día en los continuos cambios en las noticias, sino también realizar todo tipo de transacciones sin necesidad de salir de la casa. Esta situación se ha visto representada en beneficios para ciertos sectores empresariales y en retos importantes para otros, así como lo detalla en los resultados de las encuestas PriceWaterhouseCoo (PwC), la reconocida firma de consultoría, en su artículo "Securing your Tomorrow, Today. The Future of Financial Services" (2020b), en el que resalta, desde la perspectiva de los servicios financieros, cómo a largo plazo la banca aumentará su tendencia hacia el *e-commerce* de manera positiva para el sector logístico, pero de manera negativa con respecto al sector de ventas minoristas, así como de manera positiva para el sector de pagos *contactless* y móviles.

Bajo este panorama, se evidencia que el aumento del cibercrimen también irá en alza, tal como se señala en el artículo "Fighting Fraud: A Never-Ending Battle. PwC's. Global Economic Crime and Fraud Survey" de PriceWaterhouse-Coopers (2020a). En este se resalta que los delitos relacionados con fraudes de clientes y cibercrimen son los que más han aumentado, de modo que tiene el segundo una representación del 34 % en la frecuencia de la experiencia general; también resalta el reporte que "cerca de 47 % de los encuestados experimentó fraude los pasados 24 meses; lo que se reporta como el segundo nivel de incidentes más alto en los últimos veinte años". Para Latinoamérica, de acuerdo con esta tendencia, representará un reto lidiar no solo con los problemas de índole social, sino también con mejorar o implementar metodologías que ofrezcan a los usuarios de bancos, así como a las entidades, herramientas dirigidas a hacer un seguimiento adecuado a esos y otros delitos relacionados.

De igual forma, como lo afirma Aguilar (20 de mayo de 2020) en el *Diario ContraRéplica*, el país con mayor gasto en prevención de delitos financieros ha sido México, ya que dentro de su inversión para prevenir dicho tema ha invertido USD 8,4 millones, seguido de Chile, con USD 7,4 millones, Argentina con USD 6,4 millones y Brasil con USD 6,0 millones. Se dice que la inversión debe ser mayor en tecnología y no en recursos humanos, ya que las personas pueden presentar un mayor descuido en comparación con la tecnología. Sin embargo, no se trata de realizar una inversión tan alta, sino, más bien, de encontrar la eficacia de dichas herramientas y así lograr la prevención de dicho delito.

E-ISSN 2619-6301 No. 14, Año 2021

En el informe de la OEA acerca del estado de la ciberseguridad en el sector bancario en América Latina y el Caribe del 2018 se resalta que dos de los mayores riesgos para las entidades bancarias es el sabotaje a través de un *insider* (empleado insatisfecho) y el *defacement* (alteración en sitio web), con un 4,8 y 5,56 de riesgo, respectivamente, en una valoración de 1 a 7. De igual manera, se han identificado por parte de los bancos eventos relacionados con ingeniería social, *malware*, *phising*, violación de políticas de escritorio limpio, fraude interno y ataques DoS como los más altos, sobre todo en las entidades más grandes. En general, para su protección utilizan métodos tales como sistemas de detección y prevención, sistemas de gestión de identidades y accesos, sistemas de información de seguridad y gestión de eventos, sistemas de prevención de pérdida de datos, monitoreo de amenazas y vulnerabilidades, proceso de gestión de cuentas privilegiadas y evaluaciones periódicas de riesgo cibernético.

Por otra parte, el informe de ciberseguridad de América Latina y el Caribe (Banco Interamericano de Desarrollo y OEA, 2020) muestra que, en general, hay países como Ecuador y Perú que aún están desarrollando una estrategia nacional de ciberseguridad, ya que en estos la maneja, principalmente, el ejército. Una de las mejores respuestas a incidentes la presenta actualmente Uruguay, seguido de México, Colombia, Chile y Brasil, que han aumentado su respuesta al realizar la comparación entre los años 2016 y 2020.

El informe también relaciona aquellos países que no hacen parte del convenio de Budapest, el tratado internacional para el manejo de los delitos informáticos. Algunos, como México, Guatemala y Brasil, están en proceso de aceptación, mientras de otros, como, por ejemplo, Uruguay, Bolivia y Venezuela, al igual que varios de Centroamérica, se desconoce su intención de vinculación. En el caso de Colombia, recién se unió en el 2020 (Cancillería de Colombia, 2020).

Metodología

El alcance de la investigación se remite a los siguientes países de Latinoamérica: Argentina, Brasil, Bolivia, Ecuador, Chile, Colombia, Perú, Paraguay y México. Se centró en un análisis preliminar con el fin de identificar las amenazas en la red a las que se exponen los sistemas financieros en los respectivos países, así como qué están haciendo para disminuir la afectación y la representación de la informática forense en cada uno.

Se realizó la recolección de información sobre repositorios, diarios, páginas especializadas y bases de datos en línea; de igual forma, esta información recolectada se usó con el fin de sistematizar la información y realizar posteriormente el análisis correspondiente.

Resultados

Argentina

Según el artículo de Infotechnology (9 de marzo de 2020), Argentina sufrió cerca de cuatro millones de ciberataques por día en el 2019, y fueron los bancos y otras entidades relacionadas las que más riesgo presentaron. De los ataques los más relevantes se relacionaron con *botnets* y troyanos. De acuerdo con este incremento delictivo, la Asociación de

bancos de Argentina (ABA), creó campañas de concientización con sus clientes enfatizando en que ningún banco solicitará datos personales, códigos o contraseñas a sus usuarios por ningún medio electrónico.

Bajo esta tendencia al alza de los ataques, un estudio avalado por Microsoft y del cual detallan sus datos en iProUP, las tendencias en ciberseguridad para el 2020 se enfocarán en: inteligencia artificial, manejo de los datos en la nube asegurando aún más sus modalidades públicas e híbridas, así como el aumento de la seguridad en dispositivos móviles, autenticación multifactor y colaboración para identificar a tiempo las amenazas. Un aspecto a resaltar es que entre las medidas de prevención, las más comunes son los antivirus, *firewall*, antiespam con un 56 % de implementación y capacitaciones con un 36 %. Lo más preocupante es que un 27 % aún no hace ninguna inversión en seguridad.

Una entidad que se destaca en el análisis forense es Info-Lab (Laboratorio de Investigación y Desarrollo de Tecnología en Informática Forense). Ellos implementan el modelo PURI, un proceso unificado de recuperación de información que sigue unos lineamientos para llevar a cabo el proceso de análisis, manejo y recolección de la evidencia. Asimismo, dentro de las herramientas forenses que utilizan se encuentran: dd (FAU), FTK imager, LIME, HDTA2, OSFMount, VirtualBox, VMWare Workstation, RegRipper, Autopsy, CIRA y exiftool, entre otros (Info-lab, 2016).

Brasil

Para el 2019, en el periodo de enero a diciembre, el CERT de Brasil reportó 875.327 casos, entre los que se reportaron como principales incidentes el escaneo (46 %), DoS (34 %), gusanos (11 %), fraude (4 %) y ataques para comprometer servidores o desfigurar páginas web (2 %). El "escaneo", en particular, se utiliza para detectar vulnerabilidades en los equipos. Al hacer la comparación con respecto al año anterior, en el que se reportaron 676.514 incidentes, se evidencia un aumento en los incidentes. Por otra parte, el director del Comité Ejecutivo de Prevención del Fraude de Febraban (Federación Brasileña de Bancos), Adriano Volpini, señaló para el artículo de *Noomis* del 2018 que "la ingeniería social se ha convertido en el motor del fraude en Brasil", pues se considera que más del 70 % de las estafas están relacionadas con esta práctica (Rolli, 30 de enero del 2018).

Teniendo en cuenta que para el 2018, de los 78,9 billones de transacciones financieras reportadas en el país, 313,3 billones se asociaron a la banca móvil, eso representa un 24 % más con respecto al 2017 (Llanos-Small, 30 de agosto de 2019). Se buscan, por tanto, mecanismos que permitan mejorar la seguridad mediante la implementación, por ejemplo, de tecnologías de *blockchain*. Anualmente, se invierten cerca de R 24,6 mil millones en tecnología por parte de los bancos, tal como lo menciona S*ecurity Report* (enero 12 de 2021). Sin embargo, también está el foco en la educación digital, con miras a contrarrestar los

E-ISSN 2619-6301 No. 14, Año 2021

ataques de ingeniería social, así como la creación de un plan de seguridad y leyes de protección de datos (Instituto Propague, 24 de febrero de 2021; *Ciberseguridad*, 2019; GAT, s. f.; *Noomis*, 2020).

En el nivel forense para extracción de evidencias utilizan algunas herramientas como lo son: XRY, Cellebrite UFED, Solo4 y Tableau (Fernandes *et al.*, 2017). Andrade (2019) resalta que llevar a cabo los procesos de identificación, preservación, análisis y presentación de la evidencia relacionados con el internet de las cosas es un reto forense. Dado el crecimiento de la utilización de la banca móvil, como se explicaba, es relevante estar al tanto de esta información. También habla de algunas herramientas como lo son FTK y EnCase. Complementando el énfasis del análisis forense en Android, Jean (2018) habla de utilizar herramientas como AFLogical-OSE para extracción de datos, Virtualbox y Fotoforensics en el análisis de metadatos contenidos en una imagen. Otra herramienta a tener en cuenta es FD-TK-Ubuntu, con la aplicación SCALPEL (Carvalho *et al.*, 2018).

Bolivia

En el 2018 se llevó a cabo un ataque por medio de *phishing* al banco Unión S. A. Por medio de un enlace de un supuesto concurso del banco se dirigía a una web fraudulenta para robar los datos de usuario y contraseña asociados al banco real (Observatorio de Delitos Informáticos Bolivia, 2018). Por otra parte, teniendo como eje el importe de amenazas cibernéticas en Bolivia realizado por la empresa Checkpoint, el Observatorio de Delitos Informáticos Bolivia, las principales amenazas que se tienen son *malware* y *botnets*, en las que el 80 % de los archivos maliciosos en Bolivia se entregaron por correo electrónico (Observatorio de Delitos Informáticos Bolivia, 2020).

Bolivia se encuentra en el puesto 79, y es el último país de América Latina en cuanto a preparación en ciberseguridad. En Bolivia se cuenta con una agencia que se encarga de la gestión de asuntos de seguridad cibernética y gobierno electrónico, la Agencia para el Desarrollo de la Sociedad de la Información en Bolivia (ADSIB). Entre los objetivos con los que cuenta esta agencia se incluyen gestiones de coordinación para ampliar las tecnologías de la información y las comunicaciones (TIC), las cuales se realizarán mediante la sensibilización de la sociedad sobre la seguridad cibernética, la asociación en proyectos con el sector privado y la sociedad civil (Ciberseguridad, 2020). Otras sugerencias para mejorar en ciberseguridad es la educación financiera, y a futuro implementar tecnologías tales como uso de datos biométricos, la inteligencia artificial, *blockchain* y firmas electrónicas (Alba, 2020).

La empresa boliviana *YanapTI* ha participado en casos para esclarecer hechos de entidades financieras, robos de tarjetas de crédito o de débito, manipulación de cajeros automáticos, manipulación de cajas de ahorro, homicidios, análisis de celulares y casos de destrucción de información, a fin de determinar la gravedad del borrado de información. Un ejemplo se proporciona en el artículo

"Análisis documental del cómputo forense y su situación en México": se evidenció un caso de fraude en el que el gerente de una empresa realizaba el intercambio de información sensible sobre la compañía. En un análisis forense que se realizó, se logró evidenciar que los archivos que se enviaban tenían ocultos hojas de cálculo y documentos con información que probaban el delito por el cual había sido sancionado (YanapTI, 2009).

Chile

En septiembre del 2020, como lo menciona Harán (8 de septiembre de 2020), el BancoEstado de Chile sufrió uno de los más grandes ciberataques, al punto que lo obligó a cerrar todas sus oficinas y se vio obligado a asociarse, principalmente, con un *ransomware* llamado Sodinokibi. Sin embargo, como informan Solis y Fossa (2020) para el diario *Interferencia*, ya se habían presentado ataques desde junio de ese año. En un nivel general el país sufrió cerca de 525 millones de ataques durante el primer semestre del 2020 (TrenDTIC, 2 de septiembre de 2020). En Chile, las estafas más comunes están asociadas a los bancos :*vishing*, *phishing* y *skimming* (Scotiabank, 2019). Otros que también se reportan como elementos que afectan la ciberseguridad son: *whaling*, manipulación mediante d*eepfake*, ingeniería social, *spoofing* y las APT (amenazas persistentes avanzadas) (Castillo, enero 18 de 2021; Infotecs, 16 de marzo de 2021).

El país se encuentra en una expansión de las *fintech* con un crecimiento del 29 % para el 2017. Los más fuertes en este tipo de emprendimientos son Brasil, México, Colombia y Argentina (Deloitte, 2018). Esto es relevante, dado que las *fintech* se enfocan en la banca virtual, por lo que su nivel de ciberseguridad debe estar también presente en su implementación. La protección es el nuevo desafío, por lo que, como lo especifica Arenas (2021) para *BankingNew*s, las nuevas tecnologías se plantean como opciones con miras a contribuir a aumentar la seguridad a través de *deep learnig*, EDR (*endpoint detection and response*), UBA (*user-behavior analytics*), modelos seguridad del tipo Zero Trust, modelos de seguridad en *cloud* y blindaje para aplicaciones (AppShielding). Por otra parte, la última normativa dictaminada por la Comisión para el Mercado Financiero (CMF) estableció para julio del 2020 aumentar la gestión de la seguridad de la información (CMF, 2020).

En el nivel de las herramientas se podría hablar de la búsqueda de un *framework* de ciberseguridad, destacando algunas medidas de protección tales como *pinpass*, perturbador magnético, mensajería a clientes, monitoreo y prevención de fraudes (Salgado Díaz, 11 de septiembre de 2020). Céspedes (2019), por su parte, resalta aspectos de la auditoría forense para la prevención de fraudes electrónicos. Se destacan las empresas Forensic & Cybercrime Investigation, Kepler y ForensicCorp, relacionadas con el análisis forense, así como con la implementación de diversas herramientas para recuperar datos y la búsqueda de información, entre otros, siendo las herramientas Encase las más utilizadas (Forensicorp, s. f.). También se destaca el *cloud* Access Security Brocker (CASB), implementado en la empresa Kepler para monitorear la interacción de los usuarios con nubes externas o

E-ISSN 2619-6301 No. 14, Año 2021

propietarias (Kepler, s. f.). En el caso de Forensic se destaca su investigación forense también en el nivel de equipos móviles (FCI, s. f.).

Colombia

El más reciente boletín de Fortinet Threat Intelligence Insider, muestra cómo para Colombia se han realizado, durante los tres primeros meses del 2021, 6.952.587 detecciones de virus, 5.575.384 detecciones de *botnet* y 836.170.014 detecciones de *exploit* (Fortinet, 2021). También cabe destacar el más reciente ataque a la web del Congreso de la República, el 28 de abril de 2021, en el marco de las jornadas de protestas que ha vivido el país, aunque sin mayores consecuencias reportadas (Infobae, 29 de abril de 2021).

De acuerdo con un informe de Asobancaria (2020), durante el 2019 el principal delito reportado fue el hurto por medios informáticos, con cerca de 31.058 denuncias, y es probable que siga en aumento, al igual que los riesgos de terceros y el *malware* (CSIRT-Asobancaria, 8 de abril de 2021). Esto también se podría asociar con el hecho de que las *fintech* están creciendo, así como lo demuestra otro informe de Asobancaria y la OEA (2019), enfocado en el riesgo financiero: entre el 2017 y el 2018 se ha presentado un gran aumento y Colombia ocupa el tercer lugar, por debajo de México y Brasil, este último encabezando la lista. De igual manera, debido a los efectos de la pandemia, la suplantación de sitios web para capturar datos personales tuvo un crecimiento del 303 % respecto al 2019 (Ceballos *et al*., 2020), lo que enfatiza en el llamado al país para comenzar a hacer una inversión significativa en pro de la prevención e inversión en ciberseguridad.

De igual manera, en el nivel de bancos un enfoque hacia el monitoreo es innegable, tal como lo resalta Rivner (2021) en *Itnewslat*, de modo que las predicciones de ciberseguridad serán: la detección de cuentas mula, los controles de identidad, el desarrollo de las tecnologías de fraude, el seguimiento de estafas con ingeniería, el aumento del ataque de los estafadores a bancos que operan en teléfonos móviles y a las *fintech*. Sin embargo, es necesario destacar que, debido al aumento de las amenazas, la inversión en la prevención de delitos financieros ha aumentado en un 14 % en el país (ACIS, 2021). También se destaca la participación de instituciones como el Mintic, el CAI virtual de la Policía y el CSIRT de la Policía, así como en normativa el Conpes 3995 (Política Nacional De Confianza y Seguridad Digital), dirigido a aumentar el marco de seguridad e involucrar más a los usuarios. De igual forma, como lo recalcan Guerrero y Castillo (2017), un pilar fundamental para la seguridad financiera es educar.

En el nivel de informática se destaca el artículo de Muñoz *et al.* 2020, en el que se resalta el valor de la auditoría forense en tiempos del Covid-19. Asimismo, Suárez y Perea (2018) se enfocan en la importancia de las auditorías. Por otra parte, la guía para el desarrollo de una investigación en el fraude financiero propuesta por Cordero (2013), así como el análisis financiero y de seguridad informática realizado por Hernández (2014), permiten contrastar la época actual de acuerdo con la proyección que allí se planteó. El análisis forense digital

tiene su origen en el 2004, y uno de los primeros casos relacionados fue el análisis de los computadores de las FARC por parte del grupo de especialistas de informática de la Fiscalía (Jaramillo y Torres, (2016).

Ecuador

En julio del 2021 fue atacada la Corporación de Nacional de Telecomunicaciones del Ecuador. El ataque se llevó a cabo por medio de un *ransomware*. También se resalta que el Banco Pichincha en Ecuador sufrió un ataque tiempo atrás por parte del grupo de *hackers* Hotarus Corp (Loaiza, 19 de julio de 2021). El banco en un comunicado del 18 de febrero del 2021 especificó que encontraron un acceso no autorizado a los sistemas de un proveedor, y que el *modus operandi* se centró en correos fraudulentos en nombre del banco, aunque sin aparente afectación de pérdida de datos (Banco Pichincha, 2021). Según el EcuCert (equipos de respuesta a incidentes de seguridad de Ecuador), los tres principales reportes en el nivel de ciberseguridad están relacionados con *botnet*, *sinkhole* http y *scanners*, esto con respecto a los datos de los primeros seis meses del 2021 (EcuCert, 2021).

Entre los casos que se han dado en Ecuador en cuanto a delitos Informáticos, entre enero y diciembre del 2010, fueron recibidos más de 866 denuncias relacionados con delitos informáticos. De estos casos que se recibieron, 697 fueron de apropiación ilícita, 86 de delitos informáticos (vulneración a páginas de servicio público), 82 fueron a páginas de servicio privado y uno fue reportado como estafa, en el cual se usaron medios informáticos. En Ecuador estos delitos están tipificados con el Código Orgánico Integral Penal (COIP), a fin de dar seguimiento a dichos casos e implementar sanciones (Alcívar *et al.*, 2018).

Ecuador no cuenta con una normativa sobre informática forense relacionada con auditorías forenses, a diferencia de, por ejemplo, México y Perú. Por otra parte, se evidenció en el 2013 un desvió de fondos desde el Banco Central de Ecuador; a pesar de realizarse una auditoría, los resultados no permitieron encontrar a los culpables (Caraguay, 6 de febrero de 2020).

México

El SPEI es el sistema de pagos electrónicos interbancarios y la infraestructura del Banco de México. Cuenta con un sistema de seguridad que incluye contraseñas, firma digital y *tokens*, entre otros (Banco de México, 2018). Fue creado en el 2004 para permitir las transferencias entre diversos clientes (Banco de México, s. f.). En el 2018 este sistema sufrió uno de los mayores ciberataques, con una afectación cercana de cuatrocientos a ochocientos millones de pesos, lo que afectó a cinco bancos, entre ellos Citibanamex, Banorte y Banejército (*BBC mundo*, 15 de mayo de 2018). Sin embargo, ocurrieron algunas alertas antes de que se fuera efectuando el ataque, pues desde el 2017 Bancomext, Kuspit y Banejército registran evidencia de ataques previos (*Estrategia y Negocios*, 27 de mayo de 2018). Este incidente sigue presente en el sistema bancario, pero no ha tenido una respuesta clara de los responsables, aunque sí favoreció el hecho de aumentar la seguridad en este tipo de entidades (Infosecurity México, 18 de marzo de 2021; Leyva, 28 de abril de 2020).

E-ISSN 2619-6301 No. 14, Año 2021

Para el 2020 se bloquearon 324.000 amenazas por día, provenientes de correo electrónico, lo que fue equivalente a más de 118 millones (Noguez, 29 de marzo de 2021). También para ese año se han reportado ataques en usuarios de servicios financieros (Condusef), el Banco de México (Banxico) y el Sistema de Administración Tributaria (SAT) por acción de *defacement* o modificación de la página web principal, así como otro tipo de ataques como, por ejemplo, presencia de *malware* (Riquelme, 2 de enero de 2021). Es notorio que los principales incidentes ocurridos entre el 2019, el 2020 y el 2021 están relacionados con vulnerabilidades de los cajeros automáticos y *ransomware (*Leyva, 4 de junio 2021).

Para contrarrestar esta oleada de ataques se han generado mecanismos enfocados en la seguridad. Así, por ejemplo, el Banco de México creó su Centro de Defensa de Ciberseguridad (CDC), refuerza la ley de protección de datos y fortalece una estrategia de seguridad dentro del Banco de México para favorecer una mejor respuesta a incidentes (Banco de México, 2019). También se busca aumentar la presencia de profesionales en ciberseguridad, se buscan nuevas herramientas tecnológicas como *blockchain*, pero, sobre todo, en un enfoque hacia la cooperación por medio de equipos de respuesta a incidentes y capacitación del personal con miras a mantenerlo informado (Harán, 31 de mayo de 2018; Deloitte México, 21 de agosto de 2019).

Un ejemplo de la acción del análisis forense en México es el informe público que se obtuvo del evento del SPEI, en el cual se encontró que el *modus operandi* se basó en tres acciones: inserción de operaciones apócrifas (simulación de órdenes de transferencia), uso de cuentas beneficiarías válidas y eliminación de evidencias (Banco de México, 29 de agosto de 2018). La empresa Duriva se especializa en peritaje informático y entre sus servicios ofrece los relacionados con problemas en transferencias bancarias, de modo que ayuda a identificar, preservar y objetar en juicio de acuerdo con las pruebas que tengan valor (Duriva, s. f.). Por otra parte, el equipo de respuestas a incidentes de seguridad en cómputo UNAM-CERT, liderado por la Universidad Autónoma de México, específica algunas herramientas con las que han contado para el análisis forense tales como *scripts* propios, herramientas libres y gratuitas (Autopsy, Sleuthki, Foremost, Chkrootkit, RKHunter, OllyDbg), y herramientas comerciales (Encase, IDA Pro, SoftICE) (Aquino, 2005).

Paraguay

De acuerdo con el informe del estado de ciberseguridad en Paraguay del 2020, los reportes de incidentes estuvieron relacionados, principalmente, con compromiso del sistema equipo (755 reportes), seguido de *software* malicioso (*malware*) y correo no deseado malicioso (*spam*/*scam*) (531) y *phishing* (136) (Ministerio de Tecnologías de la Información y Comunicación, 2020). También para el 2020 se reportó afectación a entidades bancarias por parte de un troyano en Android llamado "Ghimob (CERT-PY, 2020).

En un informe preliminar relacionado con el plan de seguridad cibernética en el 2016, los bancos son los principales blanco para realizar ataques, por lo que la Asociación de Bancos de Paraguay (Asoban) y la Asociación de Entidades Financieras del Paraguay (Adefi) cuentan

con un comité de seguridad que les permite comunicarse; se establece que cada entidad hace campañas con sus clientes, aunque se especifica que faltan r campañas en conjunto que las integren todas (Ministerio de Tecnologías de la Información y Comunicación, 2016). Para el 2020 el Mintic de Paraguay incentivó a evitar el *phishing*, debido al auge de plataformas en línea que generó la pandemia del Covid-19 (Ministerio de Tecnologías de la Información y Comunicación, 2020). Por otra parte, un reporte reciente con respecto al manejo de las *fintech* en Paraguay establece como mecanismos de seguridad la implementación de firmas electrónicas y la firma digital (Larroza, 2021).

Una empresa que se dedica al análisis forense no solo en Paraguay, sino también en otros países de Latinoamérica, es CYBSEC Security Sytems. Entre sus actividades está el análisis de *logs*, el análisis de la información, el *cracking* de claves de archivos y la esteganografía, entre otras actividades. Algunas de sus herramientas de *software* son Encase, Forensic Toolkit, herramientas *free-ware*, así como las comerciales (CYBSEC security Sytems, s. f.). El Ministerio Público de Paraguay también cuenta con una sección de informática forense encargada de hacer la evaluación a equipos relacionados con delitos, como, por ejemplo, los celulares sobre los que se realiza hace el análisis (Ministerio Público. República del Paraguay, s. f.).

Perú

En el 2018 ocurrió un ciberataque al sistema financiero mundial que la banca peruana logró contrarrestar. Entre los mecanismos que utilizaron se identificó el *ransomware*, negación de servicio y otro por medio de un virus que se encarga de distraer el ataque (Redacción Gestión, 18 de agosto de 2018). De igual manera, la desconfianza crece para los clientes de bancos, en los que se reciben 1.800.000 quejas de usuarios cada año, y de esas quejas recibidas al año casi cinco mil al día (Vargas, 28 de octubre de 2019).

Algunos de los ataques que reporta el sector bancario son: *phishing*, *smishing*, *malware* y *man in the middle*, por lo que los bancos se enfocan en suministrar consejos para contrarrestarlos, como, por ejemplo, tener *software* actualizado, recalcar que los bancos no solicitan información relevante por medio de correos y no utilizar redes públicas para transacciones, entre otros (BBVA Perú, s. f.). Ahora bien, en noviembre del 2016 fue emitido un decreto legislativo, el n.° 1249, por el cual se fortalece el rol de Unidad de Inteligencia Financiera (UIF-Perú) en el combate del lavado de activos (LA). Estos delitos preceden el financiamiento del terrorismo (FT) (Superintendencia de Banca, Seguros y AFP-SBS Informa, 2017). También a través de los informes suministrados por el PECERT para el Gobierno peruano se hace seguimiento a incidentes informáticos (Gob.pe, s. f.).

El peritaje informático se utiliza para hacer análisis forense. Esto básicamente constituye en una investigación para la búsqueda de pruebas que sean de relevancia jurídica ante un caso (Cacha, 2019). Los requisitos que tienen en cuenta para dar validez judicial a la evidencia digital son: admisibilidad, autenticidad, integridad, fiabilidad, claridad y credibilidad (Loyola, s. f.).

E-ISSN 2619-6301 No. 14, Año 2021

Discusión de resultados

A continuación, se muestran los reportes correspondientes a los últimos tres meses del 2020 y los seis primeros del 2021 con respecto a detecciones de virus, *botnet* y *exploit*, de acuerdo con los datos suministrados por la empresa Fortinet® para los periodos Q4 2020/Q1 2021/Q2 2021, relacionados con Latinoamérica, disponibles en la página web https://www.fortiguardthreatinsider.com/es/bulletin/Q1-2021.

En la figura 1 se resumen los reportes de virus, detecciones de *botnet* y detecciones de *exploit*, de acuerdo con los reportes de Fortinet®. Para otros, no se encontraron datos en esa plataforma de manera pública, aunque no se descarta que los manejen de forma privada.

Reportes de virus

En la figura 2 se evidencia los reportes por virus. En este caso han sido mayores en Brasil y Colombia, seguidos de Perú y México, lo que revela también un crecimiento para el Q2 2021 con respecto a los dos cuartiles anteriores.

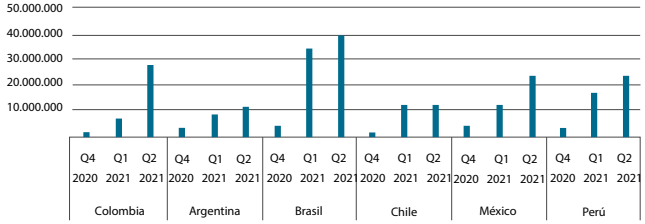
Figura 1: Reporte de detección de virus, *botnet* y *exploit* en algunos países de Latinoamérica

País	Cuartil	Detecciones virus	Detecciones de Botnet	Detecciones de exploit
Colombia	Q4 2020	1.411.994	9.381.208	1.532.065.730
	Q1 2021	6.952.587	5.575.384	836.170.014
	Q2 2021	27.753.582	31.842.678	2.659.663.035
Argentina	Q4 2020	4.408.998	2.118.982	543.535.746
	Q1 2021	9.479.086	1.177.138	113.769.672
	Q2 2021	11.438.724	5.370.207	884.527.956
Brasil	Q4 2020	4.320.726	19.794.904	4.842.361.848
	Q1 2021	34.593.274	13.354.086	3.192.856.048
	Q2 2021	40.075.545	102.509.226	12.958.076.214
Chile	Q4 2020	1.842.162	12.917.706	1.700.004.224
	Q1 2021	12.341.784	9.791.536	385.708.342
	Q2 2021	12.634.005	40.360.221	1.657.562.409
México	Q4 2020	3.381.969	27.859.346	10.550.351.567
	Q1 2021	11.865.977	16.568.626	765.695.075
	Q2 2021	23.600.964	100.309.370	60.517.975.248
Perú	Q4 2020	3.514.206	15.705.864	781.449.474
	Q1 2021	17.614.411	9.690.480	1.044.577.092
	Q2 2021	24.327.375	40.804.983	3.714.706.545

Nota. Tabla resumen que representa el conteo total hasta miles de millones de acuerdo con lo reportado para cada uno de los cuartiles Q4 2020/Q1 2021/Q2 2021.

Fuente: elaboración propia. Los datos base son tomados de la empresa Fortinet®.

Figura 2: Detecciones de virus de acuerdo a los periodos Q4 2020/Q1 2021/Q2 2021



Nota. Representación gráfica del número de virus reportados teniendo en cuenta un conteo total hasta millones.

Fuente: elaboración propia. Los datos base son tomados de la empresa Fortinet®.

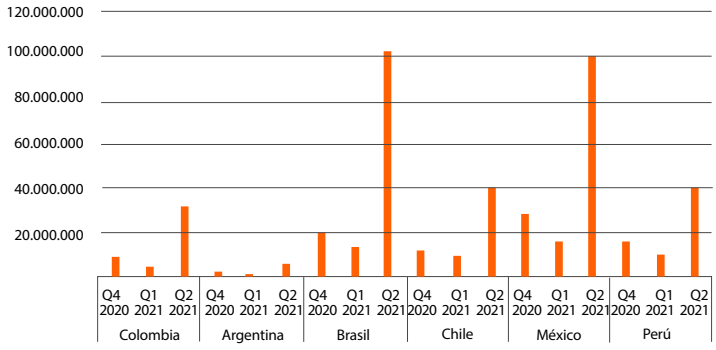
Con respecto a la familia de los virus se encuentran los troyanos, cuya función es filtrarse en el equipo que se esté usando por el usuario, para que con este acceso el delincuente cibernético acceda a toda la información relevante financiera. Estos tipos de troyanos han sido detectados sobre todo en Brasil, seguido por Perú, Argentina y Colombia. Para evitar este tipo de virus, lo que se recomienda es mantener el equipo actualizado, no ver películas en sitios no oficiales, ser cuidadosos con la información que se recibe por correo electrónico y no utilizar *cracks* (Barbosa, 3 de mayo de 2019).

Reportes botnet

En la figura 3 se encuentra que los países más afectados por *botnets* han sido Brasil y México, seguidos de Perú, Chile y Colombia. Asimismo, se evidencia que para el Q2 del 2021 sus reportes se han triplicado con respecto a los cuartiles previos.

Un ejemplo que se puede especificar es Emotet, reportado inicialmente como un troyano, pero que a lo largo del tiempo fue evolucionando hasta llegar a convertirse en un *malware* malicioso que permite descargar más códigos dañinos en los equipos de las víctimas, y así extraer información, como, por ejemplo, credenciales de los usuarios , nombres de usuarios, nombres de dominio y también llegar a instalar otro tipo de *malware*, por ejemplo TrickBot. Este *botnet* se puede filtrar por medio de correos electrónicos, archivos descargables e incluso dentro del paquete de Office, a fin de evitarlo. Se recomienda estar pendiente de los correos que llegan, mantener actualizados los equipos, deshabilitar macros de los paquetes de Office y también utilizar la herramienta de Windows EmoCheck, la cual permite saber si el equipo fue infectado por Emotet. Para más información véase Malwarebytes (s. f.).

Figura 3: Detecciones de *botnets* de acuerdo con los periodos: Q4 2020/Q1 2021/Q2 2021



Nota. Representación gráfica del número de *botnets* reportados teniendo en cuenta un conteo total hasta millones.

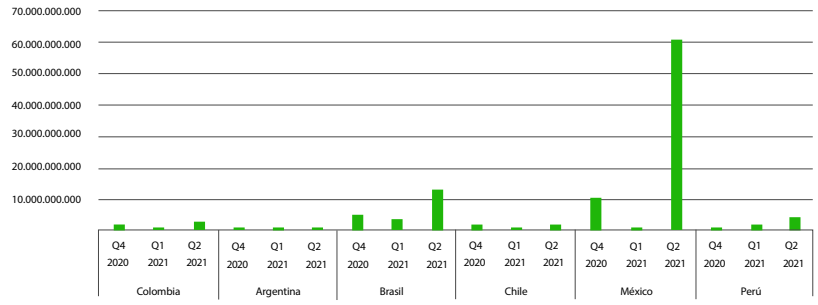
Fuente: elaboración propia. Los datos base son tomados de la empresa Fortinet®.

Reportes exploit

En la figura 4 el país con mayor afectación por *exploits* ha sido México, donde en el segundo cuartil del 2021 ha aumentado de manera significativa en comparación con los demás países evaluados.

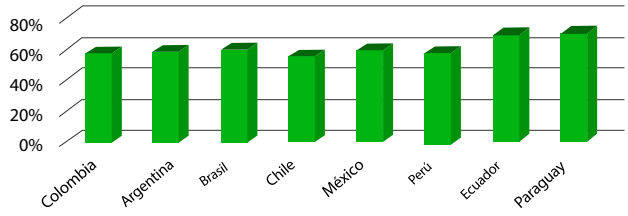
E-ISSN 2619-6301 No. 14, Año 2021

Figura 4. Detecciones de *exploits* de acuerdo con los periodos Q4 2020/Q1 2021/Q2 2021



Nota. Representación gráfica del número de *exploits* reportados teniendo en cuenta un conteo total hasta miles de millones. Fuente: elaboración propia. Los datos base son tomados de la empresa Fortinet®.

Figura 5: Porcentaje de empresas que reportaron al menos un incidente de seguridad en el 2019



Nota. Representa dentro de las empresas encuestadas el porcentaje de ellas que reportó por lo menos un tipo de incidente de seguridad.

Fuente: adaptado del informe Security Report Latinoamérica 2020/ ESET® (p. 10).

Double Pulsar y Eternal Blue son ejemplos de *exploits* detectados en Latinoamérica, aunque no son los únicos. Por otra parte, Colombia fue el tercer país más afectado en el ámbito mundial por MB/Exploit.MS17-10, con el 7 % del total de las detecciones realizadas. Para que dichos *exploits* fueran propagados se empezaron a realizar campañas de Crysis, las cuales eran dirigidas más específicamente a Colombia; esta propagación se realizó por medio de correos electrónicos que simulaban temas de deudas, de esta forma creaban duda en los usuarios y, a continuación, descargaba un documento (Bilić, 2019).

Incidentes de seguridad en empresas

En la figura 5, de acuerdo con el informe Security Report Latinoamérica 2020, al menos el 60 % de las empresas sufrió un incidente de seguridad en el 2019; los principales ataques fueron relacionados con códigos maliciosos. Es por tanto importante tener medidas de seguridad en todas las empresas, ya que el no hacerlo implicaría el hecho de una inversión mayor debido a la pérdida de información o la inactividad del sistema. Por otra parte, teniendo en cuenta que la expansión de las *fintech* seguirá en auge debido a que el sistema financiero busca ampliar su

cobertura por medio de la tecnología, a pesar del riesgo que implica por diversos ciberataques, es un camino que seguirá tomando, ya que, como se ha observado, la pandemia simplemente aceleró el proceso de transición hacia la expansión en la nube por parte de la banca.

Manejo de ciberseguridad

De acuerdo con la investigación, en la figura 6 se resume si en años recientes (menos de cinco años), el país ha reportado algún tipo de incidente, si cuenta con algún sistema de manejo de incidentes y algunos de los incidentes reportados o amenazas principalmente asociadas al sistema bancario.

Se evidencia que en años recientes se ha visto comprometido el sistema debido a ciberataques o mecanismos relacionados; a lo largo del artículo se dan más detalles de cómo ha sido esta afectación. Los CSIRT (equipo de respuesta a incidentes de seguridad informática), los CERT (equipo de respuestao preparación) para emergencias informáticas, los CIRT (equipo de respuesta a incidentes informáticos) y el SOC (centro de operaciones de seguridad) (Moyle, 2019) hacen posible organizar las respuestas en torno a la ciberseguridad, lo que permite que el país genere una acción más rápida ante un eventual incidente o amenaza, por lo que son importantes en el propósito de generar mayor control. Para hacer este seguimiento, en algunos casos se manejan como observatorios de delitos (como ocurre en Bolivia), aunque en general cumplirían la misma función.

Figura 6: Resumen con respecto al manejo de la ciberseguridad en algunos de los países de Latinoamérica

País	¿Han reportado ciberataques en años recientes recientemente?	El país cuenta con un CSIRT, CERT o similar	Principales incidentes reportados asociados con el sistema bancario y/o amenazas en ciberseguridad
Colombia	Si	Si	Botnet, virus, exploit, malware, hurto por medios informáticos
Argentina	Si	Si	Botnets, troyanos, exploit.
Brasil	Si	Si	Escaneo, DoS, gusanos , fraude, ataques para comprometer servidores o desfigurar páginas web,
Chile	Si	Si	Vishing, pishing, skimming, ransomware,whaling, ingeniería social, spoofing, APT (Amenazas persistentes avanzadas),manipulación mediante deepfake, botnet, virus, exploit.
México	Si	Si	Botnets, virus, exploit, malware, hurto por medios informáticos
Perú	Si	Si	Ransomware, negación de servicio, phishing, smishing, malware, man in the middle, botnet, virus, exploit
Bolivia	Si	Si	Malware, botnet, pishing.
Ecuador	Si	Si	Ransomware, scanners, botnet, sinkhole http
Paraguay	Si	Si	Malware, correo malicioso, pishing, troyano

Nota. Tabla resumen del análisis en ciberseguridad, teniendo en cuenta si han sufrido ataques recientes, si tienen un equipo enfocado en ciberseguridad y algunos incidentes que se han reportado.

Fuente: elaboración propia.

E-ISSN 2619-6301 No. 14, Año 2021

Figura 7: Algunas acciones recomendadas para mejorar la ciberseguridad

Algunas acciones a implementar para mejorar la seguridad
Sistemas de detección y prevención
Sistemas de gestión de identidades y accesos
Sistemas de información de seguridad y gestión de eventos
Sistemas de prevención de pérdida de datos
Monitoreo de amenazas y vulnerabilidades
Proceso de gestión de cuentas privilegiadas
Evaluaciones periódicas de riesgo cibernético
Campañas de concientización, educación digital
Aumento de la seguridad en dispositivos móviles
Autenticación multifactor
Colaboración para identificar a tiempo las amenazas
Implementar antivirus, firewall, antiespam. Mantener el software actualizado
Implementar nuevas tecnologías como blockchain, Inteligencia artificial y/o Deep learning
A nivel de cada país implementar (si no los hay) leyes de protección de datos así como leyes sobre crímenes y delitos de alta tecnología
Crear por cada empresas un plan de seguridad y políticas de seguridad
Uso de datos biométricos, controles de identidad, Firmas electrónicas
EDR (Endpoint Detection and Response)
UBA (User-behavior analytics),
Modelos Seguridad del tipo "Zero Trust",
Modelos Seguridad en "cloud"
Blindaje para Aplicaciones (AppShielding)
Utilizar Pinpass
Implementar Perturbador magnético
Monitoreo y prevención de fraudes
Detección de cuentas mula
Desarrollo de las tecnologías de fraude
Seguimiento de estafas con ingeniería
Prevención de delitos financieros
No utilizar redes públicas para transacciones
Presencia de profesionales en ciberseguridad

Nota. Tabla resumen con algunas recomendaciones para mejorar la ciberseguridad. Fuente: elaboración propia.

Se observa que se han presentado diversos incidentes, muchos relacionados con virus, *botnets* o *exploit*, como se expuso en la discusión previa, pero también se destaca lo que es el *phishing*, así como las estafas por medio de correos electrónicos. No es de extrañar esta tendencia, teniendo en cuenta que la pandemia acrecentó el auge de los servicios *online* bancarios, tal como se detalló por medio de los informes previos. Para tener en cuenta, el 2018 fue cuando se vio una afectación significativa en ataques al sistema bancario, y se afectaron en mayor medida México y Perú.

Algunas acciones recomendadas para mejorar la ciberseguridad

De acuerdo al sondeo realizado se recopila, en general, en la figura 7, algunas posibles opciones que se pueden llevar a cabo para mejorar en seguridad. Por otra parte, si bien no está especificado, se recomienda tener en cuenta la seguridad con respecto a los cajeros automáticos para evitar incidentes como el ocurrido en México, donde fue atacado el SPEI teniendo como puente este medio (*BBC mundo*, 15 de mayo de 2018).

También es importante recalcar el manejo de políticas de seguridad, planes, normas y demás componentes relacionados que permitan fortalecer esta área y evitar mayor compromiso de la información en las diversas entidades. Esto también iría de la mano de una fuerte educación digital que evite a los usuarios caer en fraudes que pongan en riesgos sus bienes y datos, así como sistemas de prevención y monitoreo en el nivel interno. Pertenecer al convenio de Budapest también favorece la comunicación entre los países integrantes para fortalecer la seguridad.

La búsqueda en la implementación de nuevas tecnologías tales como *blockchain*, inteligencia artificial o podrían constituirse a futuro como herramientas que permitan una mejor seguridad, así como una respuesta más rápida a incidentes. Por último, es recomendable un aumento en los profesionales de seguridad que favorezcan la inclusión de nuevas estrategias y la comunicación en pro del mejoramiento de la seguridad.

Relación informática forense

En la figura 8 se muestra algunas de las herramientas que se pueden implementar para investigaciones forenses. Se destaca la implementación de FTK imager y Encase entre las más comunes. Por otra parte, en algunos casos es posible desarrollar *scripts* propios como los que implementa UNAM-CERT en México (Aquino, 2005). También se evidencia un acercamiento a la seguridad en la nube, por ejemplo, por medio de Cloud Access Security Brocker (CASB) (Kepler, s. f.).

La figura 9 muestra algunas estrategias o en algunos casos los nombres de modelos que se utilizan en el nivel del análisis forense. Se destaca el hecho de cómo en algunos lugares como Perú se maneja más el concepto de peritaje para relacionarlo con la estrecha relación que tiene con la rama judicial y el seguimiento que se debe hacer para la muestra de la evidencia.

Figura 8: Algunas herramientas de *software* o *hardware* implementadas en análisis forense

Herramienas de *software/Hardware* utilizadas en análisis forense
dd (Fau), FTK imager, Lime, HTDA2, OSF-Mount, VMWare
XRY, Cellebrite UFED, Solo4, Tableau, FTK, AFLogical-OSE
Virtualbox, Fotoforensics, SCALPEL, Forensic Toolkit
Workstation, Regrigger, Autopsy, CIRA, exiftool
Encase, Cloud Access Security Brocker (CASB)
Scripts propios, Autopsy, Sleuthki, Foremost, Chkrootkit
RKHunter, OllyDbg, IDA Pro, SofICE

Nota. Tabla resumen que muestra algunas herramientas que utilizan en los diferentes países evaluados aplicados en informática forense.

Fuente: elaboración propia.

En la figura 10 se relacionan algunas entidades encargadas de realizar análisis de informática forense teniendo como valor la preservación de la información que se está manejando, a fin de estar en capacidad de recuperarla en caso de pérdida o interpretarla en caso que esta se corrompa, o la implementación de otros mecanismos que ayuden a obtener el resultado esperado. Esto es importante, ya que, así como aumenta la presencia de ataques informáticos, es relevante que más entidades y capital humano se vinculen para prevenir y hacer seguimiento

E-ISSN 2619-6301 No. 14, Año 2021

ante ese tipo de amenazas. Esto, de igual manera, amplía el campo de acción de los ingenieros que se especializan en ciberseguridad, no solo en el sector bancario, sino también, en general, en las empresas.

Figura 9: Algunos modelos/estrategias implementadas en informática forense

Algunos modelos/estrategias implementados en informática forense
Modelo PURI (proceso unificado de recuperación de información)
Análisis documental del Cómputo Forense
Técnicas de Análisis Forense
Elaboración de informes
Peritaje infórmatico
Investigación de équipos móviles
Auditorías forenses
Análisis de logs
Cracking de claves de archivos
Esteganografía
Auditoría forense
Dictamenes forenses digitales
Procesos de identificación, preservación, análisis y presentación de la evidencia

Nota. Tabla resumen que muestra algunos modelos o estrategias que utilizan en los diferentes países evaluados aplicados en informática forense.

Fuente: elaboración propia.

Figura 10: Algunas entidades relacionadas con informática forense

Algunas entidades relacionadas con informática forense	País relacionado
Info-Lab	Argentina
YanapTi	Bolivia
Forensic y Cybercrime investigation	Chile
ForensicCorp	Chile
Kepler	Chile
Ministerio Público de Paraguay	Paraguay
Duriva	México
UNAM - CERT	México
CAI virtual policia nacional	Colombia
Fiscalía	Colombia

Nota. Tabla resumen que muestra algunas entidades que aplican la informática forense en los diferentes países evaluados.

Fuente: elaboración propia.

Conclusiones

Se evidenció en la investigación cómo ha aumentado el reporte de incidentes de seguridad, lo que de un modo u otro se relaciona con la presencia de la pandemia que obligó a gran parte de la población a utilizar los servicios digitales ofrecidos por los bancos. Esto se convirtió en una oportunidad propicia para los atacantes. Los países con más ataques han sido Brasil, México, Perú, Colombia y Chile. Por otra parte, en la revisión de la base de datos de Fortinet® no se encontró reportes de asociados a virus, *exploits* o *botnets* para Bolivia y Paraguay, aunque también puede ser que esté relacionado a que no son datos que han sido autorizados de manera pública, o que, como en el caso de Bolivia, se publiquen solo en sus páginas asociadas, como es el Observatorio de Delitos Informáticos Bolivia, en el que algunos datos son realizados por otras empresas consultoras como *Checkpoint*.

Es importante enfatizar en la educación en ciberseguridad y el fortalecimiento de políticas y normas que permitan mejores acciones ante eventuales ataques, ya que, si bien los bancos han tratado de

implementar mejores canales de comunicación con sus clientes, aún falta mucho para concientizar sobre la importancia de un buen uso de los servicios financieros de una manera responsable. De igual manera, de acuerdo con las necesidades de cada empresa, establecer cuáles serían las mejores estrategias para proteger su información y, sobre todo, enfatizar en la prevención. Esto también constituye una oportunidad para afianzar la importancia de los ingenieros que manejan un enfoque en ciberseguridad. Por otra parte, las nuevas tecnologías pueden también constituir una base importante en el nivel del aumento de seguridad en el sector bancario, para que, de este modo, se brinde mayor nivel de confiabilidad a los usuarios finales.

En cada país investigado se evidenció que se están tratando de implementar diferentes leyes y formas de afrontar los delitos cibernéticos. Aunque es evidente que no en todos los países de Latinoamérica se da la misma importancia a este tema, o no se ha profundizado. Es importante que esta normativa esté en constante revisión para que pueda adaptarse a los constantes cambios, ya que los ciberdelitos, de la mano de los ciberdelincuentes, siempre van a evolucionar e identificar más vulnerabilidades. Es por tanto imprescindible hacer un seguimiento tanto en las políticas de seguridad de cada empresa como en las que se manejan en el nivel general en el país; este sería un aspecto importante sobre el cual ahondar en futuras investigaciones: cómo las leyes se han ido implementando ante el riesgo de ciberataques.

La informática forense ayuda a que los datos se mantengan protegidos y resguardados de todos aquellos ciberdelincuentes que se encuentran al acecho de cualquier descuido del empleado o la compañía para vulnerarlos, o, en su defecto, de recuperarlos en caso de ser eliminados. Son ahora una rama valiosa con gran proyección a futuro para tener en cuenta en el fortalecimiento del área de informática en las empresas y una aliada importante del sector bancario. Se encontraron algunas empresas cuyo eje central es el estudio de la informática forense; esto es importante porque abre las puertas a los especialistas en seguridad informática, sin embargo, se debe determinar si hay suficiente personal enfocado en ciberseguridad, dado el aumento exponencial de los ataques. Se cuenta también con más herramientas que ayuden en estas investigaciones, aunque igual requieren un personal calificado que no solo pueda ejecutarlas, sino también llevar a cabo un análisis adecuado y de acuerdo con modelos, estándares o protocolos que se manejan para la disposición correcta de la evidencia.

Es importante identificar en el nivel de cada banco cuáles son las principales amenazas que se pueden presentar de acuerdo con su modelo de negocio y el ambiente en el que se desarrolla. Esto les permitirá actuar con mayor eficacia en el momento de que se materialice un evento. Los sistemas de detección y monitoreo también favorecen para hacer un seguimiento ante, por ejemplo, ataques DoS. Es importante también el implementar auditorías, ya que por medio de estas se hace la evaluación del sistema

E-ISSN 2619-6301 No. 14, Año 2021

de seguridad y se puede identificar fallas en el nivel interno, pues en ocasiones el personal del banco está relacionado con otorgar accesos no autorizados, lo que a la larga compromete los activos.

En el recorrido de esta investigación fue posible evidenciar cómo en Latinoamérica el tema de los ciberdelitos crece poco a poco, y cómo las estrategias para contrarrestarlos también. Por ejemplo, México que ha sido uno de los más afectados con este tipo de sucesos, ha logrado contrarrestar estas acciones con una serie de funciones que ha ido aplicando con base en la experiencia, al igual que Chile o Brasil, aunque falta mucho por ampliar en este tema.

Agradecimientos

Agradecemos a nuestras familias por el apoyo y al Semillero de Investigación en Informática Forense, encabezado por el profesor Camilo Cardona, quien nos brindó su acompañamiento durante este proceso.

Referencias

ACIS. (2021, marzo). Empresas financieras en Colombia gastan US$180 millones al año para prevenir delitos financieros. https://bit.ly/3m6DiYO

Aguilar, J. (2020, mayo 20). México el país latinoamericano con mayor gasto en prevención de delitos financieros. *Diario ContraRéplica*. https://www.contrareplica.mx/nota-Mexico-el-pais-latinoamericano-con-mayor-gasto-en-prevencion-de-delitos-financieros-20202050

Alba, M. (2020). Banca digital en Bolivia: ciberseguridad y educación financiera. https://llamafinanciera.wixsite.com/website/post/banca-digital-en-bolivia-ciberseguridad-y-educaci%C3%B3n-financiera

Alcívar, C., Blanc, G. y Calderón, J. (2018). Aplicación de la ciencia forense en los delitos informáticos en el Ecuador y su punibilidad. *Revista Espacios*, *39*(42), 15. http://www.revistaespacios.com/a18v39n42/a18v39n42p15.pdf

Amaya, J. (2014). *El sistema financiero y la seguridad informática* (tesis de grado). Universidad Piloto de Colombia.

Análisis documental del Cómputo Forense y su situación en México. (s. f.). Capítulo 1. Antecedentes y terminología. https://bit.ly/3suwzZY

Andrade, M. (2019). Internet das Coisas: novos desafios na análise forense. *Parcerias Estratégicas*, 24(48), 33-54. https://bit.ly/3k7qsXL

Aquino, R. (2005). *Experiencias de análisis forense en México*. Departamento de Seguridad en Cómputo-UNAM-CERT UNAM. https://bit.ly/3mfP6YG

Arenas, V. (2021, enero 12). Ciberseguridad es el desafío constante de la industria financiera en Chile. *Banking News*. https://bit.ly/3AQs5zH

Asobancaria y Organización de Estados Americanos (OEA) (2019). *Desafíos del riesgo cibernético en el sector financiero para Colombia y América Latina*. https://bit.ly/3yYMG4a

Asobancaria. (2020, agosto 3). La auditoría de la ciberseguridad. *Banca & Economía*, 1244. https://bit.ly/3gdUGXT

Asociación de Bancos de Argentina (ABA). (2020, octubre 7). Todos los bancos del país se unen en una campaña para cuidar a sus clientes. https://bit.ly/37PGKPd

Banco de México. (2021). *Estrategia de ciberseguridad del banco de México*. https://www.banxico.org.mx/sistema-financiero/d/%7B1C588DE0-FC6F-5C53-E43B-2A6079957069%7D.pdf

Banco de México. (2018, agosto 29). *Reporte de análisis forense. Versión pública*. https://bit.ly/3mc33qD

Banco de México. (2018, mayo). ¿Qué es y cómo funciona el SPEI? https://bit.ly/3mhwjMR

Banco de México. (s. f.). Características del Sistema de Pagos Electrónicos Interbancarios (SPEIhttps://www.banxico.org.mx/servicios/spei_-transferencias-banco-me.html

Banco Pichincha. (2021, febrero 18). Comunicado oficial 18 de febrero 2021. https://bit.ly/3mbz81H

Barbosa, D. C. (2019, mayo 3). Troyanos bancarios en América Latina durante el primer trimestre de 2019. Welivesecurity.com. https://www.welivesecurity.com/la-es/2019/05/03/troyanos-bancarios-america-latina-primer-trimestre-2019/

BBC Mundo. (2018, 15 de mayo). México: el ciberataque "sin precedentes" a los bancos del país que causó pérdidas millonarias. //bbc.in/3k5WKSD

BBVA Perú. (s. f.). Ciberseguridad en el Perú. Bbva.pe. https://www.bbva.pe/blog/mi-seguridad/ciberseguridad-en-el-peru.html

Bilić, D. G. (2019, enero 10). Las amenazas informáticas que más afectaron a los países de América Latina. Welivesecurity.com. https://www.welivesecurity.com/la-es/2019/01/10/amenazas-informaticas-mas-afectaron-paises-america-latina/

Cacha, M. (2019). *Peritaje informático basado en una nueva metodología híbrida en 2m & J Ingenieros-Huaraz 2019* (tesis de maestría). Universidad Peruana de Ciencias e Informática. http://repositorio.upci.edu.pe/bitstream/handle/upci/137/T-CACHA_ARANA_CRISTHIAN.pdf?sequence=1&isAllowed=y

Cancillería de Colombia. (2020, marzo 17). Colombia se adhiere al Convenio de Budapest contra la Ciberdelincuencia. https://www.cancilleria.gov.co/newsroom/news/colombia-adhiere-convenio-budapest-ciberdelincuencia

Caraguay R., S. X. (2020, febrero 6). Aplicación de informática forense en auditorías gubernamentales para la determinación de indicios de responsabilidad penal con delitos informáticos en Ecuador, México y Perú, 2007-2019. *Estado & Comunes, Revista de políticas y Problemas Públicos*, *2*(11), 135-153. https://doi.org/10.37228/estado_comunes.v2.n11.2020.178

Carvalho, F., Eduardo, B. y Rodrigues, A. (2018). Computação forense: uma aplicação de softwares livres para recuperação de dados digitais. *Revista Eletrônica Argentina-Brasil de Tecnologias da Informação e da Comunicação*, *1*(9). 10.5281/zenodo.1478921 https://revistas.setrem.com.br/index.php/reabtic/article/view/300

Castillo, A. (2021, enero 18). Los siete ciberataques a los que hay que ponerles atención este 2021 en Chile. *PWC*. https://www.pwc.com/cl/es/prensa/prensa/2021/Los-siete-ciberataques-a-los-que-hay-que-ponerles-atencion-este-2021-en-Chile.html

Ceballos, A., Bautista, F. y Mesa, L. (2020). *Ciberseguridad en entornos cotidianos. Tic-Tac*. Cámara Colombiana de Informática y Telecomunicaciones (CCIT). https://www.ccit.org.co/wp-content/uploads/ciberseguridad-en-entornos-cotidianos-vfene-1.pdf

Centro de Respuestas ante Incidentes Cibernéticos (CERT-PY). (2020). Troyano bancario en Android llamado "Ghimob" dirigido a aplicaciones financieras, afecta a Paraguay. Cert.gov.py. https://www.cert.gov.py/noticias/troyano-bancario-en-android-llamado-ghimob-dirigido-aplicaciones-financieras-afecta-paraguay

Cert.Br. (2020). Estatísticas dos Incidentes Reportados ao CERT.br. Centro de Estudos, Res-

E-ISSN 2619-6301 No. 14, Año 2021

posta e Tratamento de incidentes de Segurança no Brasil. https://www.cert.br/stats/incidentes/

Centro de Respuestas ante Incidentes Cibernéticos (CERT-PY). (2020). Troyano bancario en Android llamado "Ghimob" dirigido a aplicaciones financieras, afecta a Paraguay. https://www.cert.gov.py/noticias/troyano-bancario-en-android-llamado-ghimob-dirigido-aplicaciones-financieras-afecta-paraguay

Céspedes, R. (2019). Análisis de los elementos de seguridad utilizados por una institución bancaria para prevenir fraudes electrónicos en transacciones de igual naturaleza, en relación con la auditoría forense. *Revista de Investigación Aplicada en Ciencias Empresariales*, *4*(1), 7. 10.22370/riace.2015.4.1.1868. ResearchGate. https://bit.ly/3k2KYbP

Ciberseguridad. (2019). Ciberseguridad. Noticias relevantes sobre este sector en auge. https://ciberseguridad.com/normativa/latinoamerica/brasil/

Ciberseguridad. (2020). Ciberseguridad Bolivia. https://ciberseguridad.com/normativa/latinoamerica/bolivia/#:~:text=El%20Gobierno%20de%20Bolivia%20no,trav%C3%A9s%20del%20ArCERT%20de%20Argentina.

Comisión para el Mercado Financiero (CMF). (2020, julio 7). En bancos e instituciones financieras: CMF publica normativa para la gestión de la seguridad de la información y ciberseguridad. Cmfchile.cl. https://www.cmfchile.cl/portal/prensa/615/w3-article-29314.html

Consejo Nacional de Política Económica y Social. (2020, julio 1). Conpes 3995: Política Nacional de Confianza y Seguridad Digital. https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3995.pdf

Cordero, E (2013). *Análisis forense para caso de fraude en los sistemas de información transaccional de una entidad financiera* (tesis de grado). Universidad Piloto de Colombia. http://repository.unipiloto.edu.co/handle/20.500.12277/3016

Salgado Díaz, S. (11 de septiembre de 2020). Hacia *un framework* para la ciberseguridad en la banca. Creasys.cl. https://www.creasys.cl/hacia-un-framework-para-la-ciberseguridad-en-la-banca/

CSIRT-Asobancaria. (2021, abril 8). Informe de tendencias de ciberseguridad "Navigating Cyber 2021". https://bit.ly/2VWL64h

CYBSEC. (s. f). Análisis informático forense. Cybsec.com. http://www.cybsec.com/ES/servicios/cursos/sem13py.php

Deloitte. (2018, noviembre). Creando valor en la gestión de riesgos en la industria financiera. *Revista Perspectivas*. https://www2.deloitte.com/content/dam/Deloitte/cl/Documents/risk/El%20estado%20de%20la%20ciberseguridad%20en%20las%20instituciones%20financieras_2.pdf

Deloitte México. (2019, agosto 21). Ciberataques financieros. ¿Cómo enfrentar esta amenaza? Deloitte.com. https://www2.deloitte.com/mx/es/pages/dnoticias/articles/ciberataques-financieros-en-mexico.html

Duriva (s. f.). Transferencias bancarias. *Peritaje Informático*. https://peritajeinformatico.com.mx/servicios/transferencias-bancarias/

EcuCert. (2021). EcuCert de Arcotel. Estadísticas. Ecucert.gob.ec. https://www.ecucert.gob.ec/estadisticas/

ESET. (2020). Security Report. Latinoamérica 2020. https://www.welivesecurity.com/wp-content/uploads/2020/08/ESET-Security-Report-LATAM_2020.pdf

Estrategia y Negocios. (2018, mayo 27). México: banca resiste cinco ciberataques en un mes. https://www.estrategiaynegocios.net/finan-

zas/1182018-330/m%C3%A9xico-banca-resiste-cinco-ciberataques-en-un-mes

Fernandes, K., Eduardo Branco, J. y Cardoso, V. (2017). O uso da informática na perícia criminal e suas ferramentas. *Revista Espacios*, 38(51), 25.

Forensic & Cybercrime Investigation (FCI). (s. f.). Análisis forense de equipos móviles. Fci.cl. https://fci.cl/informatica-forense-y-evidencia-digital/#fraude

Forensiccorp. (s. f.). Forense. Guidance Software. Forensiccorp.cl. https://www.forensiccorp.cl/es/forensic.php

Fortinet. (2021). ColombiaQ1-2021. Fortinet Threat Intelligence Insider. Boletines para América Latina. Fortiguardthreatinsider.com. https://www.fortiguardthreatinsider.com/es/bulletin/Q1-2021

Fortinet. (s. f.). Bases de datos para Latinoamérica para los periodos Q4 2020/Q1 2021/Q2 2021. Fortiguardthreatinsider.com. https://www.fortiguardthreatinsider.com/es/bulletin/Q1-2021

GAT. (s. f.). 10 processos de Cibersegurança para fintechs: IF, IP, PIX, BACEN 4658 e 3909. Get Ahead of Threats. https://www.gat.digital/blog/ciberseguranca-para-fintechs/

Gob.Pe. (s. f.). Alerta integrada de seguridad digital del PECERT. https://www.gob.pe/institucion/pcm/colecciones/791-alerta-integrada-de-seguridad-digital-del-pecert

Guerrero, B. y Castillo D. (2017). *Desafíos técnicos y jurídicos frente al ciberdelito en el sector bancario colombiano* (tesis de grado). Universidad Nacional Abierta y a Distancia. https://repository.unad.edu.co/bitstream/handle/10596/13387/52498805.pdf?sequence=5&isAllowed=y

Harán, J (2018, mayo 31). El después del ciberataque a bancos de México: los desafíos que plantea la ciberseguridad. Welivesecurity.com. https://www.welivesecurity.com/la-es/2018/05/31/despues-ciberataque-bancos-mexico-desafios-plantea-ciberseguridad/

Harán, J. (2020, septiembre 8). Ataque de ransomware afecta a BancoEstado en Chile. Welivesecurity.

Infobae. (2021, abril 29). Web del Congreso de la República fue objeto de ciberataques. https://www.infobae.com/america/colombia/2021/04/29/web-del-congreso-de-la-republica-fue-objeto-de-ciberataques/

Info-Lab. (2016, abril). *Guía integral de empleo de la informática forense en el proceso penal* (2a ed.). Universidad Fasta. http://redi.ufasta.edu.ar:8080/xmlui/bitstream/handle/123456789/1592/PAIF.pdf?sequence=1

Infosecurity México. (2021, marzo 18). La evolución de ciberataques en la industria financiera. Infosecuritymexico.com. https://www.infosecuritymexico.com/es/articulos/la-evolucion-de-ciberataques-en-la-industria-financiera.html

Infotechnology. (2020, marzo 9). Los bancos argentinos, en peligro: reciben 4 millones de ataques por día y las pérdidas podrían ser millonarias. Cronista.com. https://www.cronista.com/infotechnology/online/Los-bancos-argentinos-en-peligro-reciben-4-millones-de-ataques-por-dia-y-las-perdidas-podrian-ser-millonarias-20200309-0007.html

Infotecs. (2021, marzo 16). APT: amenaza persistente avanzada. Infotecs.mx. https://infotecs.mx/blog/apt_amenaza_persistente_avanzada.html

Instituto Propague. (2021, febrero 24). Cibersegurança: Bancos apostam na educação digital para evitar fraudes. Institutopropague.org. https://institutopropague.org/noticias/ciberseguranca-bancos-apostam-na-educacao-digital-para-evitar-fraudes/

iProUP. (2020, febrero 5). Informe de Microsoft: 29 % de las empresas en Argentina reconoció haber sido víctima de ciberataques. Iproup.com. https://www.iproup.com/innovacion/11133-informe-de-microsoft-29-de-las-empresas-en-argentina-reconocio-haber-sido-victima-de-ciberataques

E-ISSN 2619-6301 No. 14, Año 2021

Jaramillo, D. y Torres, M. (2016). *Estado del análisis forense digital en Colombia* (tesis de grado). Universidad Militar Nueva Granada. https://repository.unimilitar.edu.co/bitstream/handle/10654/14401/TorresMoncadaMarthaLiliana2016.pdf?sequence=1&isAllowed=y

Jean, A. (2018). *Computação forense em dispositivos com sistema operacional android*. Universidade Federal do Pará Campus Universitario de Castanhal-Faculdade De Computação-Curso De Bacharelado Em Sistemas De Informação.

Kepler (s. f.). ¿Qué es Cloud Access Security Brocker (CASB)? Kepler.cl. https://kepler.cl/producto/cloud-access-security-brocker-casb/

Larroza, N. (2021). *Regulación fintech en Paraguay*. https://www.pj.gov.py/ebook/monografias/nacional/administrativo/Nabila-Larroza-Regulacion-Fintech-en-Paraguay.pdf

Leyva J. (2020, abril 28) ¿Dónde están los culpables del ataque al SPEI? *El Financiero.* https://www.elfinanciero.com.mx/opinion/jeanette-leyva/donde-estan-los-culpables-del-ataque-al-spei/

Leyva, J (2021, junio 4). Reconoce Banxico 16 hackeos a bancos. *El Financiero*. https://www.elfinanciero.com.mx/economia/2021/06/04/reconoce-banxico-16-hackeos-a-bancos/

Llanos-Small, K. (2019, agosto 30). Los retos de la ciberseguridad financiera en Brasil. *Iupana*.

Loazai, Y. (2021, julio 19). Un ataque informático apagó las computadoras de la Corporación Nacional de Telecomunicaciones del Ecuador. Infobae.com. https://www.infobae.com/america/america-latina/2021/07/19/un-ataque-informatico-apago-las-computadoras-de-la-corporacion-nacional-de-telecomunicaciones-del-ecuador/

Loyola, T (s. f.). *Cadena de custodia en los delitos computacionales e informáticos. Requisitos para su admisión y valoración de la pericia de cómputo y análisis digital forense*. https://www.mpfn.gob.pe/escuela/contenido/actividades/docs/2500_tema_07caden_cust_deli_infor_mp2_23abri.pdf

Malwarebytes. (s. f.) Emotet. Mmalwarebytes.com. https://es.malwarebytes.com/emotet/

Ministerio de Tecnologías de la Información y Comunicación. (2020). *Estado de la ciberseguridad en Paraguay año 2020*. https://www.cert.gov.py/application/files/7616/1521/7981/Informe_Ciberseguridad_Paraguay_2020_-_final-2.pdf

Ministerio de Tecnologías de la Información y Comunicación. (2016, abril 6). *Plan Nacional de Ciberseguridad. República del Paraguay*. https://www.senatics.gov.py/application/files/7114/6227/9918/Plan_Nacional_de_Seguridad_Cibernetica_v3.docx

Ministerio Público. República del Paraguay. (s. f.). Preguntas sobre laboratorio forense. Ministeriopublico.gov.py. https://ministeriopublico.gov.py/preguntas-sobre-laboratorio-forense-

Moyle, E. (2019, julio). CERT vs. CSIRT vs. SOC: ¿cuál es la diferencia? *TechTarget*. https://searchdatacenter.techtarget.com/es/consejo/CERT-vs-CSIRT-vs-SOC-Cual-es-la-diferencia

Muñoz. H., Canabal, J., Galindo, S. Zafra, B. y Benítez, Y. (2020). Informática Forense y Auditoría. *Revista Espacios*, *41*(42). 10.48082/espacios-a20v41n42p32

Noguez, R. (2021, marzo 29). Covid-19 detona ciberataques en México: hasta 4 amenazas por segundo vía mail. *Forbes*. https://www.forbes.com.mx/ciberataques-4-por-segundo-mexico-2020/

Noomis. (2020, septiembre 18). Bancos reforçam conscientização contra crimes cibernéticos na pandemia.

Observatorio de Delitos Informáticos Bolivia. (2018, octubre 22). Ataque de Phishing a Banco Unión S. A. Odibolivia.org. https://www.odibolivia.org/2018/10/22/ataque-de-phishing-a-banco-union-s-a/

Observatorio de Delitos Informáticos Bolivia. (2020, abril 23). Estado de las amenazas cibernéticas en Bolivia. Odibolivia.org. https://www.odibolivia.org/2020/04/23/estado-de-las-amenazas-ciberneticas-en-bolivia/

Organización de Estados Americanos (OEA). (2018). *Estado de la ciberseguridad en el sector bancario en América Latina y el Caribe*. Programa de Ciberseguridad del Comité Interamericano contra el Terrorismo. https://www.oas.org/es/sms/cicte/sectorbancariospa.pdf

PriceWaterhouseCoopers (2020a). *Fighting Fraud: A Never-Ending Battle. PwC's Global Economic Crime and Fraud Survey.* PwC.

PriceWaterhouseCoopers (2020b). *Securing Your Tomorrow, Today. The Future of Financial Services*. https://www.pwc.com/gx/en/financial-services/pdf/pwc-the-future-of-financial-services.pdf

Redacción Gestión. (2018, agosto 18). Ciberataque a bancos peruanos: ¿cómo se habría originado? Gestion.pe. https://gestion.pe/economia/ciberataque-bancos-habria-originado-241908-noticia/?ref=gesr

Riquelme, R. (2021, enero 2). 2020, en 12 hackeos o incidentes de seguridad en México. *El Economista*. https://www.eleconomista.com.mx/tecnologia/2020-en-12-hackeos-o-incidentes-de-seguridad-en-Mexico-20210102-0007.html

Rivner, U. (2021). Las 5 principales predicciones de ciberseguridad para 2021. *Itnews.lat*. https://itnews.lat/las-5-principales-predicciones-de-ciberseguridad-para-2021.html

Rolli, C. (2018, enero 30). Bancos em alerta. *Noomis CIAB FEBRABAN*.

Scotiabank. (2019, abril). Estafas por internet: Las tres más comunes en Chile. Scotiabankchile.cl. https://www.scotiabankchile.cl/Personas/Asesores-Financieros/Ciberseguridad-Scotia/estafas-por-internet-mas-comunes

Security Report. (2021, enero 12). Cibersegurança segue na agenda tecnológica dos bancos para 2021. Securityreport.com.br. https://www.securityreport.com.br/overview/ciberseguranca-segue-na-agenda-tecnologica-dos-bancos-para-2021/#.YGnvbOj0mUl

Solis, C. y Fossa, L. (2020, septiembre 10). Querella confirma que BancoEstado ya había sufrido grave ataque cibernético en junio. *Diario Interferencia*.

Suárez, S. y Perea M. (2018). *Auditoría forense como herramienta en la detección del fraude financiero*. Universidad Cooperativa de Colombia, Santa Marta. https://repository.ucc.edu.co/bitstream/20.500.12494/7980/1/2018_auditoria_deteccion_fraude.pdf

Superintendencia de Banca, Seguros y AFP-SBS Informa. (2017, marzo). *Mejores herramientas para combatir el lavado de activos y el financiamiento del terrorismo. Estándares GAFI y OCDE*. https://www.sbs.gob.pe/Portals/0/jer/BOL-QUINCENAL/20170316_Bol-Quincenal-N4.pdf

TrendTIC. (2020, septiembre 2). Chile sufrió más de 525 millones de intentos de ciberataques en el primer semestre del 2020. *Tendencias Tecnológicas y Negocios*.

Vargas, J. (2019, octubre 28). Perú: el sistema financiero deja cinco mil afectados al día. *Ojo Público*. https://bit.ly/3APrZIv