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[1], Daniel Andrey Hernández Ladino[2]

RESUMEN

El sistema bancario ha expandido sus servicios fuera de la planta física tomando mayor auge en la plataforma web y móvil, por lo que 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 en algunos de los países Latinoamérica, se buscó identificar si los bancos se han visto expuestos a algún tipo de amenaza en años recientes asociados con su auge en la nube, que medidas de prevención han tomado o han buscado implementar para contrarrestarlas y cuál es la contribución que ofrece o puede ofrecer la informática forense para 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.

Objetivo

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 está entrando a una nueva era hacia un cambio de paradigma tanto como lo fueron el surgimiento del renacimiento o la primera revolución industrial, debido a la afectación de impacto global que ha sido la presencia de la pandemia de Covid-19. Esta situación ha generado que las personas centren su atención hacia los medios informáticos que permiten no sólo mantenerse al día de los continuos cambios en noticias sino también realizar todo tipo de transacciones sin necesidad de salir de la casa. Dicha situación se ha visto representada en beneficios para ciertos sectores empresariales y en retos importantes para otros, así como lo especifican en los resultados de las encuestas PriceWaterhouseCoo (PwC) reconocida firma de consultoría en su artículo: *"The future of financial services"* del año 2020 donde resaltan para la perspectiva de los servicios financieros, que a largo plazo, la banca aumentará su tendencia hacia el e-commerce de manera positiva para el sector logístico pero de manera negativa para el sector de ventas minoristas, así como también de manera positiva para el sector de pagos contactless y móviles.

Bajo este panorama, también se evidencia que el aumento de cibercrimen también irá en alza, así como lo detallan en el artículo "*Global Economic Crime and Fraud Survey"* de

1 Estudiante, Ingeniería de sistemas, Fundación Universitaria del Área Andina,mareavalo31@estudiantes.areandina.edu.co

2 Estudiante, Ingeniería de sistemas, Fundación Universitaria del Área Andina, dhernandez142@estudiantes.areandina.edu.co

PriceWaterhouseCoopers, (2020) resaltando que los delitos relacionados con fraudes de clientes y cibercrimen son los que más han aumentado teniendo 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 a 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 para hacer un seguimiento adecuado a esos y otros delitos relacionados.

De igual forma, como lo dice Aguilar, J. (2020) para 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 8.4 millones de dólares, seguido por Chile, con 7.4 millones de dólares, Argentina con 6.4 millones de dólares y Brasil con 6.0 millones de dólares, 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 de encontrar la eficacia de dichas herramientas para así lograr la prevención de dicho delito.

En el informe de la OEA acerca del estado de la ciberseguridad en el sector bancario en América Latina y el Caribe del año 2018 resalta que dos de los mayores riesgos para 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 de una valoración de 1 a 7. De igual manera, se ha 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 aquellas entidades más grandes. En general, para su protección utilizan métodos 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 otro lado, en el informe de ciberseguridad de América Latina y el Caribe (Banco interamericano de desarrollo, OEA, 2020) muestra que en general hay países como Ecuador y Perú que aún están desarrollando una estrategia nacional de ciberseguridad ya que en ellos se maneja principalmente por 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 2016 y 2020. El informe también relaciona aquellos países que no hacen parte del convenio de Budapest, el cual es el tratado internacional para el manejo de los delitos informáticos. Algunos como México, Guatemala y Brasil están en proceso de aceptación mientras otros como Uruguay, Bolivia y Venezuela al igual que varios de centro América se desconoce su intención de vinculación. En el caso de Colombia, recién se unió en el año 2020 (Cancillería de Colombia, 2020).

METODOLOGÍA

El alcance de la investigación estuvo relacionado con algunos países de Latinoamérica como son: Argentina, Brasil, Bolivia, Ecuador, Chile, Colombia, Perú, Paraguay y México. Se centró en un análisis preliminar para identificar las amenazas en la red a las que se exponen los sistemas financieros en los respectivos países, que 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 para sistematizar la información para hacer posteriormente el análisis relacionado.

RESULTADOS

Argentina

Según el artículo de Infotechnology, 2021 Argentina sufrió cerca de 4 millones de ciberataques por día en el año 2019, siendo 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 a 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 año 2020 se enfocarán en: inteligencia artificial, manejo de los datos en la nube asegurando aún más sus modalidades públicas e híbridas, así como aumento de la seguridad en dispositivos móviles, autenticación multifactor y colaboración para identificar a tiempo las amenazas. Un aspecto para resaltar es que de 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 que es proceso unificado de recuperación de información el cual sigue unos lineamientos para llevar a cabo el proceso de análisis, manejo y recolección de la evidencia. Así mismo, dentro de las herramientas forenses que utilizan se encuentran: dd (FAU), FTK imager, LIME, HDTA2, OSFMount, VirtualBox, VMWare Workstation, RegRipper, Autopsy, CIRA, exiftool entre otros (Info-lab, 2016).

Brasil

Para el año 2019 en el periodo de enero a diciembre, el CERT de Brasil reportó 875.327 casos teniendo 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 donde se reportaron 676.514 incidentes se evidencia un aumento en los incidentes. Por otro lado, 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" esto porque se considera que más del 70% de las estafas están relacionadas con ingeniería social (Rolli, C., 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 año 2017 (Llanos-Small, K. 2019), se busca por tanto mecanismos que permitan mejorar la seguridad implementando por ejemplo tecnologías de blockchain. Anualmente, se están invirtiendo cerca de R $ 24,6 mil millones de reales en tecnología por parte de los bancos como lo mencionan en security report, 2021, pero también está el foco en la educación digital

para contrarrestar los ataques de ingeniería social, así como la creación de un plan de seguridad y leyes de protección de datos (Instituto propague, 2021; noomis, 2020; ciberseguridad, 2019; GAT, S.F).

A nivel forense para extracción de evidencias utilizan algunas herramientas como son: XRY, Cellebrite UFED, Solo4 y Tableau (Fernandes, et al. 2017). Andrade, M. 2019 resalta que llevar a cabo los procesos de identificación, preservación, análisis y presentación de la evidencia relacionado con el internet de las cosas, son un reto forense y dado el crecimiento de la utilización de la banca móvil como se explicaba anteriormente, 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, A. 2018 habla de utilizar herramientas como AFLogical-OSE para extracción de datos, virtualbox y Fotoforensics para el análisis de metadatos contenidos en una imagen. Otra herramienta para tener en cuenta es FDTK-Ubuntu con la aplicación SCALPEL (Carvalho, F., Eduardo, B., y Rodrigues, A, 2018

Bolivia

En el año 2018 se llevó a cabo un ataque por medio de pishing 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 otro lado, 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, donde el 80% de los archivos maliciosos en Bolivia se entregaron por correo electrónico (Observatorio de delitos informáticos Bolivia, 2020).

Bolivia se encuentra dentro del puesto 79 siendo 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 cual es la agencia para el desarrollo de la sociedad de la información en Bolivia (ADSIB). Dentro de los objetivos con los que cuenta esta agencia se incluyen gestiones de coordinación para ampliar las tecnologías de la información y comunicaciones (TIC), la cual será realizada 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, así como a futuro implementar tecnologías como uso de datos biométricos, inteligencia artificial, blockchain, firmas electrónicas (Alba, M (2020)).

La empresa boliviana *YanapTI*, ha sido participe 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 y así poder determinar la gravedad del borrado de información. Un ejemplo en el artículo Análisis documental del Cómputo Forense y su situación en México: se evidenció un caso de fraude en donde 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 de 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, J., 2020, el *BancoEstado* de Chile sufrió uno de los más grandes ciberataques que lo obligó a cerrar todas sus oficinas y se asoció

principalmente con un ransomware llamado Sodinokibi; sin embargo, como informan Solis y Fossa, 2020 para el diario Interferencia, ya se habían presentado ataques desde el mes de junio de ese año. A nivel general el país sufrió cerca de 525 millones de ataques durante el primer semestre del 2020 (TRENDTIC, 2020). En Chile, las estafas más comunes están asociadas a los bancos están: vishing, phishing y skimming (Scotiabank, 2019). Otros que también se reportan como elementos que afectan la ciberseguridad son: whaling, manipulación mediante deepfake, ingeniería social, spoofing y las APT (Amenazas persistentes avanzadas) (Castillo, 2021 para PWC; Infotecs, 2021).

El país se encuentra en una expansión de las fintech teniendo un crecimiento del 29% para el año 2017 siendo los más fuertes en este tipo de emprendimientos Brasil, México, Colombia y Argentina, así como lo reporta 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 BankingNews, las nuevas tecnologías se plantean como opciones para 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 Seguridad en "cloud"y blindaje para Aplicaciones (AppShielding). Por otro lado, la última normativa dictaminada por el CMF (Comisión para el mercado financiero) estableció para julio de 2020 con la finalidad de aumentar la gestión de la seguridad de la información (CMF, 2020).

A nivel de herramientas se podría hablar de la búsqueda de un framework de ciberseguridad destacando algunas medidas de protección como: pinpass, perturbador magnético, mensajería a clientes, monitoreo y prevención de fraudes (Creasys,2020). Céspedes, 2019 resalta aspectos de la auditoría forense para la prevención de fraudes electrónicos. Por otro lado, se destacan las empresas Forensic & Cybercrime Investigation, Kepler y ForensicCorp relacionadas con análisis forense, así como la implementación de diversas herramientas para recuperar datos, búsqueda de información entre otros siendo las herramientas Encase las más utilizadas (Forensicorp, S.F). Se destaca el cloud Access Security Brocker (CASB) implementado en la empresa Kepler para monitorear la interacción de los usuarios con nubes externas o propietarias (Kepler, S.f). En el caso de forensic se destaca su investigación forense también a nivel de equipos móviles (FCI, s.f).

Colombia

El más reciente boletín de Fortinet Theat intelligence insider, muestra como para Colombia se ha hecho 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 es de destacar el más reciente ataque a la web del congreso de la república el 28 de abril de 2021, dentro de las jornadas de protestas que ha vivido el país, aunque sin mayores consecuencias reportadas (Infobae, 2021).

De acuerdo con un informe 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 dado al igual que los riesgos de terceros y el malware (CSIRT-Asobancaria, 2021). Esto también se podría asociar con el hecho que las fintech están creciendo, así como lo demuestra otro informe de Asobancaria & OEA (2019) enfocado en el riesgo financiero donde entre el 2017 al 2018 se ha presentado un gran aumento estando Colombia en 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 A., Bautista F. y Mesa L. (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, a nivel de bancos un enfoque hacia el monitoreo es innegable, así como lo resalta Rivner, U. (2021) en Itnewslat donde las predicciones de ciberseguridad serán: La detección de cuentas mula, los controles de identidad, desarrollo de las tecnologías de fraude, seguimiento de estafas con ingeniería, aumento del ataque de los estafadores a bancos que operan en teléfonos móviles y a las fintech. Sin embargo, hay que destacar que ya 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 las instituciones como 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) para aumentar el marco de seguridad e involucrar más a los usuarios, así como lo recalcan Guerrero, B. y Castillo, D. (2017) que un pilar fundamental para la seguridad financiera es educar.

A nivel de informática se destaca el artículo de Muñoz, et. al 2020 resaltando el valor de la auditoría forense en tiempos del COVID-19 al igual que Suarez, S. & Perea, M. (2018) también enfocado en la importancia de las auditorías. Por otro lado, la guía para el desarrollo de una investigación en el fraude financiero propuesta por Cordero, E, (2013) así como el análisis financiero y de seguridad informática hecho por Hernández, J. (2014) para contrastar con la época actual de acuerdo a la proyección que allí se planteó. El análisis forense digital tiene su origen en el año 2004 siendo uno de los primeros casos tomados relacionados con el análisis de los computadores de las FARC por parte del grupo de especialistas de informática de la fiscalía (Jaramillo, D. y Torres, M. (2016)).

Ecuador

En julio de 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 también había sufrido un ataque tiempo atrás por parte del grupo de hackers Hotarus Corp (Loaiza, Y. 2021). El banco en un comunicado del 18 de febrero de 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 a nivel de ciberseguridad están relacionados con botnet, sinkhole http y scanners esto con respecto a los datos de los primeros seis meses del año 2021 (EcuCert, 2021).

Entre los casos que se han dado en Ecuador en cuanto a delitos Informáticos, entre enero a diciembre del año 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 los cuales son vulneración a páginas de servicio público, 82 fueron a páginas de servicio privado y 1o que fue reportado como estafa en el cual se usaron medios informáticos. En Ecuador dichos delitos, están tipificados con el Código Orgánico Integral Penal (COIP), está para dar seguimiento a dichos casos y dar sanciones. (Alcívar C., Blanc G. y Calderon J., 2018)

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

México

El SPEI es el sistema de pagos electrónicos interbancarios y es la infraestructura del *Banco de México*. Cuenta con un sistema de seguridad que incluye contraseñas, firma digital, 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 año 2018 este sistema sufrió uno de los mayores cibertaques con una afectación cercana de 400 a 800 millones de pesos afectando a cinco bancos entre ellos Citibanamex, Banorte y Banejército (BBC mundo, 2018). Sin embargo, ocurrieron algunas alertas antes que se fuera efectuando el ataque desde el año 2017 a Bancomext, Kuspit y Banejército donde se evidencian ataques previos (Estrategia y negocio, 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, 2021; Leyva, J. 2020)

Para el año 2020 se bloquearon 324.000 amenazas por día provenientes de correo electrónico lo que fue equivalente a más de 118 millones (Noguez, 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, también ocurrieron otro tipo de ataques como presencia de malware (Riquelme, R. 2021). Es notorio también que dentro de los principales incidentes entre 2019, 2020 y 2021 están relacionados con vulnerabilidades de los cajeros automáticos y ransomware (Leyva, J. 2021).

Para contrarrestar esta oleada de ataques se han generado mecanismos enfocados en la seguridad por ejemplo el Banco de México creó su Centro de Defensa de Ciberseguridad (CDC), se refuerza la ley de protección de datos se fortalece una estrategia de seguridad dentro del Banco de México para favorecer una mejor respuesta a incidentes (Banco de México, 2019). También se busca el aumentar la presencia de profesionales en ciberseguridad, en buscar 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 para mantenerlo informado (Harán, J. 2018; Deloitte México, 2019)

Un ejemplo de la acción del análisis forense en México es el informe público que se obtuvo del evento del SPEI donde 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, 2018). La empresa Duriva se especializa en peritaje informático y dentro de sus servicios están los relacionados con problemas en transferencias bancarias ayudando a identificar, preservar y objetar en juicio de acuerdo a las pruebas que tengan valor (Duriva, s.f). Por otro lado, 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 como son: scripts propios, herramientas libres y gratuitas (Autopsy, Sleuthki, Foremost, Chkrootkit, RKHunter, OllyDbg), herramientas comerciales (Encase, IDA Pro, SoftICE) (Aquino, R. 2005).

Paraguay

De acuerdo con el informe del estado de Ciberseguridad en Paraguay del año 2020, los reportes de incidentes estuvieron relacionados principalmente con compromiso del sistema /equipo con 755 reportes, seguido de software malicioso (malware) y correo no deseado malicioso (spam/scam) con 531 y phishing con 136 (Ministerio de Tecnologías de La Información y

Comunicación, 2020). También para el año 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 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 falta realmente campañas en conjunto que las integren todas (Ministerio de Tecnologías de La Información y Comunicación, 2016). Para el año 2020 Mintic de Paraguay incentivo para evitar el phising debido al auge de plataformas en línea debido al COVID-19 (Ministerio de Tecnologías de La Información y Comunicación, 2020). Por otro lado, un reporte reciente con respecto al manejo de las fintech en Paraguay establece como algunos mecanismos de seguridad la implementación de firmas electrónicas y firma digital (Larroza, N. 2021).

Una empresa que se dedica al análisis forense no solo en Paraguay sino en otros países de lationomérica es CYBSEC security Sytems la cual dentro de las actividades que realiza está el análisis de logs, análisis de la información, cracking de claves de archivos, esteganografía entre otras actividades. Dentro de las herramientas de software están 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 tales como por ejemplo celulares sobre los cuales se hace el análisis. (Ministerio Público. República del Paraguay, S.F).

Perú

En el año 2018 ocurrió un ciberataque al sistema financiero mundial del cual, la banca peruana logró contrarrestar. De los mecanismos que utilizaron se identificaron el ransomware, negación de servicio y otro por medio de un virus que se encarga de distraer el ataque (Redacción Gestión, 2018). De igual manera, la desconfianza crece para los clientes de bancos donde se reciben 1'800.000 quejas de usuarios cada año, y de esas quejas recibidas al año, casi cinco mil al día. (Vargas, J., 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 el 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). Por otro lado, en noviembre del 2016 fue emitido un decreto legislativo el cual es el N°1249, este decreto fortalece el rol de Unidad de Inteligencia Financiera (UIF-Peru) en el combate del lavado de activos (LA), estos delitos preceden y el financiamiento del terrorismo (FT) (Superintendencia de Banca, Seguros y AFP, 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, M., 2019). Los requisitos que tienen en cuenta para dar validez judicial de la evidencia digital son: admisibilidad, autenticidad, integridad, fiabilidad, claridad y credibilidad (Loyola, T. S.F).

DISCUSIÓN DE RESULTADOS

A continuación, se muestran los reportes correspondientes a los últimos tres meses del año 2020 y los seis primeros del 2021 con respecto a detecciones de virus, botnet y exploit de acuerdo a los datos suministrados por la empresa Fortinet® para los periodos Q4 2020/ Q1 2021/Q2 2021 relacionados con Latinoamérica disponibles en: 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 a los reportes de Fortinet®. Para otros, no se encontraron datos en esa plataforma de manera pública, aunque no se descarta que los manejen de manera privada.

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 propia**.** Los datos base son tomados de la empresa *Fortinet*®.

Reportes de Virus

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

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 propia**.** Los datos base son tomados de la empresa *Fortinet*®.

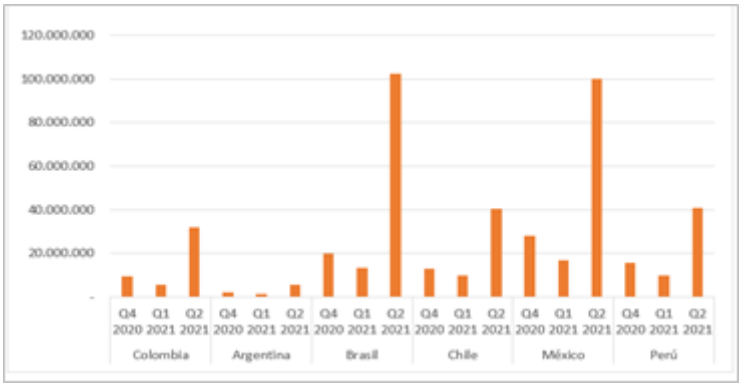
Con respecto a la familia de los virus están los troyanos, cuya función es filtrarse en el equipo que se esté usando por el usuario, para que con este acceso el delincuente cibernético, tenga acceso a toda la información relevante financiera, estos tipos de troyanos han sido detectados mayormente en 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, 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. Así mismo, se evidencia que para el Q2 del 2021 sus reportes se han triplicado con respecto a los cuartiles previos.

Figura 3

Detecciones de botnets de acuerdo a 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 propia**.** Los datos base son tomados de la empresa *Fortinet*®.

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 el cual permite descargar más códigos dañinos en los equipos de las víctimas, permitiendo extraer información como credenciales de los usuarios , nombres de usuarios, nombres de dominio y también llegar a instalar otro tipo de malware , como por ejemplo el caso de TrickBot .Este Botnet, se puede filtrar por medio de correos electrónicos, archivos descargables e incluso dentro del paquete de Office, para evitar este tipo de botnet, lo que se recomienda es 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. Más información en Malwarebytes (S.F).

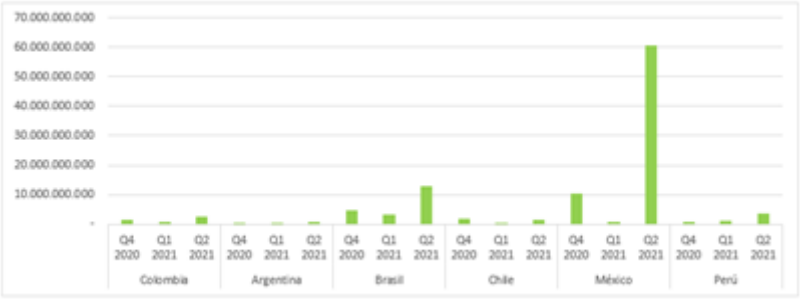
Reportes exploit

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 a comparación de los demás países evaluados.

Double Pulsar y Eternal Blue, son ejemplos de exploits detectados en Latinoamérica, aunque no son los únicos. Por otro lado, Colombia fue el tercer país más afectado a nivel 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, dicha propagación era realizada por medio de correos electrónicos que simulaban temas de deudas, de esta forma creaban duda en los usuarios y a continuación los mismos descargaba un documento (Bilić, 2019)

Figura 4.

Detecciones de exploits de acuerdo a los periodos: Q4 2020/Q1 2021/Q2 2021

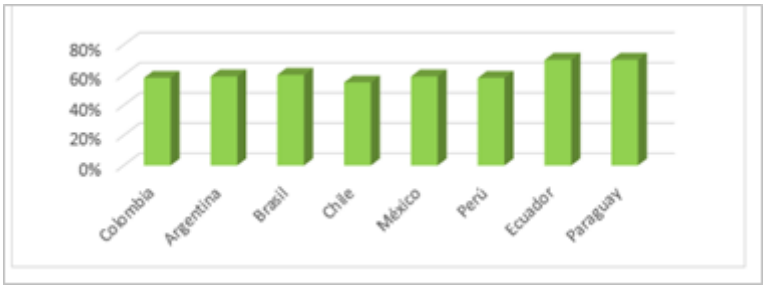


Nota. Representación gráfica del número de exploits reportados teniendo en cuenta un conteo total hasta miles de millones. Fuente propia**.** Los datos base son tomados de la empresa *Fortinet*®.

Incidentes de seguridad en empresas

Figura 5.

*Porcentaje de empresas que reportaron al menos un incidente de seguridad en el año 2019***.**



Nota. Representa dentro de las empresas encuestadas el porcentaje de ellas que reportó por lo menos un tipo de incidente de seguridad. Adaptado del informe Security Report Latinoamérica 2020/ ESET® (p. 10)

En la **figura 5** y de acuerdo con el informe Security Report Latinoamérica 2020, al menos el 60% de las empresas sufrió un incidente de seguridad en 2019 siendo los principales ataques 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 otro lado, 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.

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: propia.

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), CERT (equipo de respuesta (o preparación) para emergencias informáticas), CIRT (equipo de respuesta a incidentes informáticos) y SOC (centro de operaciones de seguridad) (Moyle, E., 2019), permiten organizar las respuestas entorno 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 para 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.

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

Algunas acciones recomendadas para mejorar la ciberseguridad

De acuerdo al sondeo hecho se recopila en general, en la **figura 7,** algunas posibles opciones que se pueden llevar a cabo para mejorar en seguridad. Por otro lado, si bien no está especificado, si 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, 2018).

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: Propia.

También es importante recalcar en 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 permita que los usuarios caigan en fraudes que pongan en riesgos sus bienes y datos, así como sistemas de prevención y monitoreo a nivel interno. El 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 como blockchain, inteligencia artificial o Deep Learning también 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 favorezcan la comunicación en pro del mejoramiento de la seguridad.

Relación informática forense

Figura 8.

Algunas herramientas de software o hardware implementadas en análisis forense

Herramientas de software/hardware utlizadas en análisis forense
dd (FAU), FTK imager, LIME, HDTA2, OSFMount, VMWare
XRY, Cellebrite UFED, Solo4, Tableau, FTK, AFLogical-OSE,
virtualbox, Fotoforensics, SCALPEL, Forensic Toolkit
Workstation, RegRipper, Autopsy, CIRA, exiftool
Encase, cloud Access Security Brocker (CASB)
Scripts propios, Autopsy,Sleuthki, Foremost, Chkrootkit
RKHunter,OllyDbg, IDA Pro, SoftICE

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

En la **figura 8** se muestran algunas de las herramientas que se pueden implementar para investigaciones forenses. Destacan la implementación de FTK imager y Encase dentro de las más comunes. Por otro lado, en algunos casos se pueden desarrollar scripts propios como los que implementa UNAM-CERT en México (Aquino, R. 2005) y 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 algunos casos los nombres de modelos que utilizan a 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 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 infórmático
Investigación de équipos móviles
Auditorías forenses
Análisis de logs
Cracking de claves de archivos
Esteganografía
Auditoría forense
Dictámenes 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: Propia

Figura 10.

Algunas entidades relacionadas con informática forense

Algunas entidades relacionadas con informática forense	País relacionado
Info-Lab	Argentina
YanapTI	Bolivia
Forensic & Cybercrime Investigation	Chile
Kepler	Chile
ForensicCorp	Chile
Ministerio público de Paraguay	Paraguay
Duriva	México
UNAM-CERT	México
CAI virtual policía nacional	Colombia
Fiscalía	Colombia

Nota. Tabla resumen que muestra algunas entidades que aplican la informática forense en los diferentes países evaluados. Fuente: 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 para poder recuperarla en caso de pérdida o interpretarla en caso que esta se corrompa, así como 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 ante ese tipo de amenazas. Esto de igual manera, amplía el campo de acción para los ingenieros que se especializan en ciberseguridad no solo en el sector bancario sino en general en las empresas.

CONCLUSIONES

Se evidenció en la investigación como 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, lo que se convirtió en una oportunidad propicia para ser aprovechada por los atacantes. Los países con más ataques han sido: Brasil, México, Perú, Colombia y Chile. Por otro lado, 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 estén relacionado a que no son datos que han sido autorizados de manera pública o que como en el caso de Bolivia, que se publiquen solo en sus páginas asociadas como es el Observatorio de delitos informáticos Bolivia donde algunos datos son realizados por otras empresas consultoras como *Checkpoint*.

Es importante enfatizar en la educación en ciberseguridad, 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 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 otro lado, las nuevas tecnologías pueden también constituir una base importante a 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 estar evolucionando al ir identificando más vulnerabilidades. Es por tanto imprescindible hacer un seguimiento tanto en las políticas de seguridad de cada empresa, así como en las que se manejan a nivel general en el país; este sería un aspecto importante sobre al cual ahondar en futuras investigaciones en el 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 de empleado o compañía para vulnerarlos, o en su defecto, a 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 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 a nivel de cada banco cuales son las principales amenazas que se pueden presentar de acuerdo con su modelo de negocio y el ambiente en el cual se está desarrollando, esto les permitirá actuar con mayor eficacia al momento 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 a través de estas se hace la evaluación del sistema de seguridad y se pueden identificar fallas a nivel interno dado que en ocasiones personal del banco está relacionada con el otorgar accesos no autorizados, que a la larga comprometen los activos.

En el recorrido de esta investigación, se pudo evidenciar como en Latinoamérica el tema de los ciberdelitos ha ido creciendo poco a poco y como las estrategias para contrarrestar los mismos también. Por ejemplo, México que ha sido uno de los más afectados con este tipo de sucesos ha logrado contrarrestar este tipo de acciones con una serie de funciones que han 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, el cual nos brindó su acompañamiento durante este proceso.

REFERENCIAS

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

Aguilar, J. (20 de mayo de 2020). 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. Recuperado de: https://llamafinanciera.wixsite.com/website/post/banca-digital-en-bolivia-ciberseguridad-y-educaci%C3%B3n-financiera

Alcívar C., Blanc G. y Calderon J. (2018). Aplicación de la ciencia forense en los delitos informáticos en el Ecuador y su punibilidad. Vol. 39 (No 42). Pag. 15. Revista espacios. http://www.revistaespacios.com/a18v39n42/a18v39n42p15.pdf

Amaya, J. (2014). El sistema financiero y la seguridad informática. Universidad Piloto de Colombia. [Tesis, Universidad Piloto de Colombia]. Repositorio institucional https://bit.ly/3iUvBTu

Análisis documental del Cómputo Forense y su situación en México. (s.f.). Capítulo 1. Antecedentes y terminología. Consultado 17 de agosto de 2021. https://bit.ly/3suwzZY

Andrade, M. (2019) Internet das Coisas: novos desafios na análise forense. Parc. Estrat. • Brasília-DF • v. 24 • n. 48 • p. 33-54 • jan-jun • 2019. https://bit.ly/3k7qsXL

Aquino, R. (2005) Experiencias de análisis forense en México. Departamento de Seguridad en Cómputo / UNAM-CERT UNAM, México. Jornadas de Análisis Forense. Madrid, España. Septiembre 2005. https://bit.ly/3mfP6YG

Arenas, V. (12 de enero de 2021). Ciberseguridad es el desafío constante de la industria financiera en Chile. Banking News. Consultado 17 de agosto de 2021. https://bit.ly/3AQs5zH

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

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

Asociación de bancos de Argentina. (ABA), (octubre 7 2020). Todos los bancos del país se unen en una campaña para cuidar a sus clientes. Consultado 17 de agosto 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 (29 de agosto, 2018) Reporte de análisis forense. Versión pública. https://bit.ly/3mc33qD

Banco de México (mayo de 2018) ¿Qué es y cómo funciona el SPEI? Consultado 17 de agosto de 2021 https://bit.ly/3mhwjMR

Banco de México (s.f) Características del Sistema de Pagos Electrónicos Interbancarios (SPEI). Consultado 17 de agosto de 2021: https://www.banxico.org.mx/servicios/spei_-transferencias-banco-me.html

Banco Pichincha (18 de febrero de 2021). Comunicado oficial 18 de febrero 2021. Comunicados oficiales. Consultado 17 de agosto de 2021. https://bit.ly/3mbz81H

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

BBC Mundo (15 de mayo de 2018) México: el ciberataque "sin precedentes" a los bancos del país que causó pérdidas millonarias. Consultado 17 de agosto de 2021. https://bbc.in/3k5WKSD

BBVA Perú (S.F). Ciberseguridad en el Perú. Consultado el 17 de agosto de 2021. https://www.bbva.pe/blog/mi-seguridad/ciberseguridad-en-el-peru.html

Bilić, D. G. (10 de enero de 2019). Las amenazas informáticas que más afectaron a los países de América Latina. Welivesecurity. 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. Universidad peruana de ciencias e informática. Escuela de posgrado. Para optar al grado académico de maestro en gestión tecnológica de la información.[Tesis de grado] http://repositorio.upci.edu.pe/bitstream/handle/upci/137/T-CACHA_ARANA_CRISTHIAN.pdf?sequence=1&isAllowed=y

Cancillería de Colombia (17 de marzo 2020) 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. (6 de febrero de 2020). 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). doi:10.5281/zenodo.1478921 https://revistas.setrem.com.br/index.php/reabtic/article/view/300

Castillo, A. (18 de enero 2021). Los siete ciberataques a los que hay que ponerles atención este 2021 en Chile. PWC, Chile. Consultado 17 de agosto de 2021. 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. TicTac. Cámara Colombiana de informática y telecomunicaciones (CCIT). https://www.ccit.org.co/wp-content/uploads/ciberseguridad-en-entornos-cotidianos-vfene-1.pdf

Cert.Br (2020) Estatísticas dos Incidentes Reportados ao CERT.br. Centro de Estudos, Resposta e Tratamento de incidentes de Segurança no Brasil. Consultado 17 de agosto 2021 https://www.cert.br/stats/incidentes/

CERT-PY (Centro de respuestas ante incidentes cibernéticos), (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. DOI: 10.22370/riace.2015.4.1.1868. ResearchGate. https://bit.ly/3k2KYbP

Ciberseguridad (2019). Ciberseguridad. Noticias relevantes sobre este sector en auge. Brasil. Consultado 17 de agosto de 2021. https://ciberseguridad.com/normativa/latinoamerica/brasil/

Ciberseguridad. (2020). Ciberseguridad Bolivia. Consultado 17 de agosto. 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) (7 de julio 2020). En Bancos e Instituciones Financieras: CMF publica normativa para la Gestión de la Seguridad de la Información y Ciberseguridad. Comisión para el mercado financiero. Consultado 17 de agosto de 2021. https://www.cmfchile.cl/portal/prensa/615/w3-article-29314.html

CONPES 3995 (1 de julio de 2020). Política Nacional de Confianza y Seguridad Digital. Consejo Nacional de Política Económica y social. 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. Universidad Piloto de Colombia. Repositorio institucional. http://repository.unipiloto.edu.co/handle/20.500.12277/3016

Creasys (2020). Hacia un framework para la ciberseguridad en la banca. https://www.creasys.cl/documentos/noticias/Creasys_Ciberseguridad_en_la_Banca_2020.pdf

CSIRT-Asobancaria (8 de abril de 2021). Informe de tendencias de ciberseguridad "Navigating Cyber 2021" realizado por FS-ISAC para el fortalecimiento de la ciberseguridad del sector. https://bit.ly/2VWL64h

CYBSEC, (S.f). Análisis informático forense. Consultado el 17 de agosto de 2021. http://www.cybsec.com/ES/servicios/cursos/sem13py.php

Deloitte (noviembre de 2018). 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, (21 de agosto de 2019). Ciberataques financieros ¿Cómo enfrentar esta amenaza? https://www2.deloitte.com/mx/es/pages/dnoticias/articles/ciberataques-financieros-en-mexico.html

Duriva (s.f) Transferencias bancarias. Peritaje informático. Consultado 17 de agosto de 2021. https://peritajeinformatico.com.mx/servicios/transferencias-bancarias/

EcuCert (2021). EcuCert de Arcotel. Estadísticas. Consultado 17 de agosto de 2021. 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 (27 de mayo de 2018) México: Banca resiste cinco ciberataques en un mes. https://www.estrategiaynegocios.net/finanzas/1182018-330/m%C3%A9xico-banca-resiste-cinco-ciberataques-en-un-mes

Fernandes, K., Eduardo Branco, J. & Cardoso, V. (2017) O uso da informática na perícia criminal e suas ferramentas. Revista espacios. Vol. 38 (No 51) pág. 25). https://www.revistaespacios.com/a17v38n51/a17v38n51p25.pdf

Forensic & Cybercrime Investigation (FCI), (s.f). Análisis forense de equipos móviles. Forensic & cybercrime investigation. Consultado 17 de agosto de 2021. https://fci.cl/informatica-forense-y-evidencia-digital/#fraude

Forensiccorp (S.F). Forense. Guidance software. Consultado el 17 de agosto de 2021. https://www.forensiccorp.cl/es/forensic.php

Fortinet (2021). ColombiaQ1-2021. Fortinet Threat Intelligence Insider. Boletines para América Latina. 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. Consultado el 17 de agosto de 2021. 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. Consultado 17 de agosto de 2021. https://www.gat.digital/blog/ciberseguranca-para-fintechs/

Gob.Pe (S.F). Alerta integrada de seguridad digital del PECERT. Colecciones. Consultado el 17 de agosto de 2021. 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. Universidad Nacional Abierta y a Distancia. Escuela de ciencias básicas tecnología e ingeniería. [Tesis. Universidad Nacional Abierta y a Distancia] https://repository.unad.edu.co/bitstream/handle/10596/13387/52498805.pdf?sequence=5&isAllowed=y

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

Harán, J. (8 de septiembre de 2020). Ataque de ransomware afecta a BancoEstado en Chile. Welivesecurity. https://www.welivesecurity.com/la-es/2020/09/08/ataque-ransomware-afecta-bancoestado-chile/
https://revistas.iaen.edu.ec/index.php/estado_comunes/article/view/178

Infobae (29 de abril de 2021). 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 (abril de 2016). Guía integral de empleo de la informática forense en el proceso penal. Segunda edición. Universidad FASTA. Mar del Plata, Argentina. http://redi.ufasta.edu.ar:8080/xmlui/bitstream/handle/123456789/1592/PAIF.pdf?sequence=1

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

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

Infotecs (16 de marzo de 2021). APT Amenaza Persistente Avanzada. https://infotecs.mx/blog/apt_amenaza_persistente_avanzada.html

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

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

Jaramillo, D. y Torres, M. (2016). Estado del análisis forense digital en Colombia. Universidad Militar Nueva Granada. Bogotá, D.C. Colombia. Trabajo de grado. 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. https://bdm.ufpa.br:8443/jspui/bitstream/prefix/2173/1/TCC_ComputacaoForenseDispositivos.pdf

Kepler (S.F). ¿Qué es Cloud Access Security Brocker (CASB)? Consultado 17 de agosto de 2021. https://kepler.cl/producto/cloud-access-security-brocker-casb/

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

Leyva J. (28 de abril de 2020) ¿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 (4 de junio de 2021) 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. (30 de agosto 2019) Los retos de la ciberseguridad financiera en Brasil. Iupana. https://iupana.com/opinion_post/los-retos-de-la-ciberseguridad-financiera-en-brasil/

Loazai, Y (19 de julio de 2021). Un ataque informático apagó las computadoras de la Corporación Nacional de Telecomunicaciones del Ecuador. Infobae. Quito. 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. Consultado el 17 de agosto de 2021. https://www.mpfn.gob.pe/escuela/contenido/actividades/docs/2500_tema_07caden_cust_deli_infor_mp2_23abri.pdf

Malwarebytes (s.f) Emotet. Consultado el 18 de agosto de 2021. 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. (6 de abril de 2016). Plan Nacional de Ciberseguridad. República del Paraguay. Borrador. Consultado 17 de agosto de 2021. 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. Consultado el 17 de agosto de 2021. https://ministeriopublico.gov.py/preguntas-sobre-laboratorio-forense-

Moyle, E. (2 de julio 2019). 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. & Benítez, Y. (2020). Informática forense y auditoría forense: Nuevas perspectivas en tiempos de COVID-19. Revista espacios. Vol. 41 (42) 2020, Art. 32, Especial COVID-19. DOI: 10.48082/espacios-a20v41n42p32. https://www.revistaespacios.com/a20v41n42/a20v41n42p32.pdf

Noguez, R. (marzo 29 de 2021) 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 (18 de septiembre de 2020). Bancos reforçam conscientização contra crimes cibernéticos na pandemia. Noomis CIAB FEBRABAN. https://noomis.febraban.org.br/temas/seguranca/bancos-reforcam-conscientizacao-contra-crimes-ciberneticos-na-pandemia

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

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

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 (2020). Fighting fraud: A never-ending battle. PwC's Global Economic Crime and Fraud Survey. https://www.pwc.com/gx/en/forensics/gecs-2020/pdf/global-economic-crime-and-fraud-survey-2020.pdf

PriceWaterhouseCoopers (2020). Securing your tomorrow, today. The future of financial services. Recuperado en: https://www.pwc.com/gx/en/financial-services/pdf/pwc-the-future-of-financial-services.pdf

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

Riquelme, R. (2 de enero de 2021). 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. Consultado el 17 de agosto de 2021. https://itnews.lat/las-5-principales-predicciones-de-ciberseguridad-para-2021.html

Rolli, C. (30 de enero de 2018). Bancos em alerta. Noomis CIAB FEBRABAN. Noomis. https://noomis.febraban.org.br/temas/seguranca/bancos-em-alerta

Scotiabank (abril 2019). Estafas por internet: Las 3 más comunes en Chile. https://www.scotiabankchile.cl/Personas/Asesores-Financieros/Ciberseguridad-Scotia/estafas-por-internet-mas-comunes

Security Report (12 de enero de 2021) Cibersegurança segue na agenda tecnológica dos bancos para 2021. Consultado el 17 de agosto de 2021. https://www.securityreport.com.br/overview/ciberseguranca-segue-na-agenda-tecnologica-dos-bancos-para-2021/#.YGnvbOj0mUl

Solís, C. y Fossa, L. (10 de septiembre de 2020). Querella confirma que BancoEstado ya había sufrido grave ataque cibernético en junio. Diario Interferencia. https://interferencia.cl/articulos/querella-confirma-que-bancoestado-ya-habia-sufrido-grave-ataque-cibernetico-en-junio

Suarez, S. & 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. (marzo de 2017). 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_BolQuincenal-N4.pdf

TrendTIC (2 de septiembre de 2020). Chile sufrió más de 525 millones de intentos de ciberataques en el primer semestre del 2020. Tendencias tecnológicas y negocios. https://www.trendtic.cl/2020/09/chile-sufrio-mas-de-525-millones-de-intentos-de-ciberataques-en-el-primer-semestre-del-2020/

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