La influencia de la automatización inteligente en la detección del cibercrimen financiero

The influence of intelligent automation on the detection of financial cybercrimen

URL: https://revistas.uta.edu.ec/erevista/index.php/bcoyu/article/view/1462

Juan Chávez-Bravo[1]; Darwin Malpartida-Márquez[2]; Armando Villacorta-Cavero[3]; Juan Orellano-Antúnez[4]

Fecha de recepción: 25 de noviembre de 2020 Fecha de aceptación: 19 de noviembre de 2021

Resumen

El presente artículo tiene como objetivo, revisar la producción científica sobre la influencia de la automatización inteligente en la capacidad para detectar los crímenes financieros. El método es de naturaleza descriptiva, se va a ocupar de describir eventos y hechos acontecidos sin encargarse de hacer predicciones o correlaciones, se ha realizado una búsqueda de información en las principales bases de datos relacionados al objetivo. El resultado de la investigación permite apreciar que la automatización inteligente resulta ser estratégico para la gestión de riesgos de fraude, ya que con análisis de tecnologías avanzadas aumenta la detección de crímenes financieros y por lo tanto hay una disminución de las pérdidas económicas. Como conclusión la transformación de la gestión de riesgos de fraude con análisis de tecnologías avanzadas genera un incremento en la detección de crímenes financieros y una disminución de las pérdidas por crímenes financieros. La transformación de la gestión de riesgos se solventa en tres cimientos asociados con el análisis avanzado: i) Integrando gran cantidad de fuentes de información de alta calidad, ii) Técnicas de modelos más sofisticados, y iii) Tecnologías de automatización inteligente como la robótica.

Palabras clave: Ataques cibernéticos, inteligencia artificial, crímenes financieros, cibercrimen financiero.

Abstract

This article aims to review the scientific production on the influence of intelligent automation on the ability to detect financial crimes. The method is descriptive in nature, it will take care of describing events and events that occurred without making predictions, correlations or predictions, a search for information has been carried out in the main databases related to the objective. The result of the research allows us to appreciate that intelligent automation turns out to be strategic for the management of fraud risks, since with advanced technology analysis, the detection of financial crimes increases and therefore there is a decrease in economic losses. As conclusion the transformation of fraud risk management with advanced technology analysis generates an increase in the detection of financial crimes and a decrease in losses due to financial crimes. The transformation of risk management is solved on three foundations associated with advanced analysis: i) Integrating a large number of high-quality information sources, ii) More sophisticated modeling techniques, and iii) Intelligent automation technologies such as robotics.

Keywords: Cyber-attacks, artificial intelligence, financial crimes, financial cybercrime.

[1] *Universidad Peruana de Ciencias Aplicadas. Escuela Profesional de Contabilidad. Lima-Perú. E-mail: juancchav@gmail.com. ORCID: http://orcid.org/0000-0002-8493-5414*
[2] *Universidad Nacional Agraria de la Selva. Escuela Profesional de Contabilidad. Tingo María-Perú. E-mail: jose.malpartida@unas.edu.pe. ORCID: https://orcid.org/0000-0001-5227-7384*
[3] *Universidad Nacional Mayor de San Marcos. Facultad de Contabilidad. Lima-Perú. E-mail: avillacorta@unmsms.edu.pe. ORCID: http://orcid.org/0000-0003-3464-7593*
[4] *Universidad Nacional Mayor de San Marcos. Facultad de Contabilidad. Lima-Perú. E-mail: jorellanoa@unmsms.edu.pe. ORCID: http://orcid.org/0000-0001-6055-4433*

Introducción

Debido al desarrollo tecnológico, las formas de fraudes cibernéticos se han sofisticados, vulnerando cualquier tipo de sistema de control interno y generando pérdidas económicas a las compañías (Bilbao, García, & Rios, 2009, pág. 3). Esto permite comentar, que en la actual época de pandemia los crímenes financieros representan sin lugar a duda una amenaza latente que debería tener muy alertas a todas las organizaciones empresariales para prevenir y detectar posibles violaciones a su sistema de seguridad de la información. Es así como, en las empresas, se hace indispensable prestar atención a los ataques cibernéticos causados a los sistemas, ya que pueden generar problemas potenciales de alto riesgo donde podrían ser víctimas de crímenes financieros.

Para Guerrero y Castillo (2017) el auge de la globalización y la tecnología ha creado un ciberespacio en el cual encontramos un sin números de recursos y plataformas que han ayudado al desarrollo de la actividad humana, no obstante, también está el aspecto negativo como la ciberdelincuencia que están generando en las organizaciones y los gobiernos el replanteamiento de las estrategias para combatir estos delitos prospectivamente. Los bancos o entidades financieras son más susceptibles a estos tipos de ataques cibernéticos, debido a que "la materia prima con la que se prestan los servicios bancarios es el dinero. Estas circunstancias propician la aparición de casos de fraude y exponen a los bancos a la realización de estafas" (Arcenegui-Rodrigo, Obrero-Castilla, & Martín-Lozano, 2016, pág. 627). Es decir, Los delincuentes cibernéticos viajan por el mundo virtual y realizan incursiones fraudulentas cada vez más y con mayor frecuencia y mayor impacto, los dispositivos de almacenamiento y procesamiento de información llámense servidores, estaciones de trabajo o simplemente PC son vulnerados en sus elementos más sensibles, dejando expuestos no sólo múltiples y significativos datos de distinto valor (financiero, crediticio, estratégico, productivo), sino los mismos patrimonios reales de personas y organizaciones y, aún más, su dignidad, su honra y su vida (Ojeda & Arias, 2010, pág. 45).

Arocena (2012) señala que "*en los tiempos que corren, las nuevas tecnologías, en general, y la informática, en particular, introducen incansablemente no sólo nuevas formas de realizar tareas conocidas, sino también nuevas actividades, muchas de las cuales se manifiestan como antisociales y reprobables*" (pág. 946).

Según Abaimov y Martellini (2017) el producto de actividades delictivas, dan nacimiento a estas organizaciones criminales que se encuentran totalmente intercomunicadas, generando astronómicas cantidades de dinero a estos ciberdelincuentes con ganancias que bordean los 1,5 trillones de dólares anuales. Asimismo, se indica que 23% de las empresas fueron víctimas de algún incidente de ciberseguridad en los últimos 12 meses, teniendo como agente principal ocasionado por el malware o software malicioso (51%) el incidente más cotidiano, detrás se encuentra la denominada suplantación de identidad de proveedores o de personas vía correo electrónico institucional (41%), acontecimiento denominado como business email compromise (p.1).

Asimismo, importantes foros y expertos revelan que:

- Los Ciberataques son el sexto riesgo global con mayor probabilidad de ocurrir (Global Risk Report 2020).
- Ocho de cada 10 vulneraciones se detectan dentro de las 24 horas (estadísticas del Gobierno del Reino Unido, reveladas en la Revista Auditor Interno (agosto del 2016).

Sin embargo:

> Si los clientes y empresas no ven el entorno digital como un espacio confiable y seguro para la realización de sus interacciones, la desconfianza afectaría el uso de los canales digitales y por lo tanto todas las inversiones realizadas en procesos de digitalización de la experiencia del cliente no generaría el impacto positivo esperado (Organización de los Estados Americanos, 2019, pág. 18).

Estos acontecimientos no son ajenos en empresas peruanas y no es raro notar que han tenido ataques de ciberseguridad que tiene efectos económicos y que finalmente tendrá un impacto en la sostenibilidad de las empresas en el mediano y largo plan. En un artículo publicado por la agencia peruana de noticias (Pichihua, S., 2018) relacionados a crímenes financieros perpetrados, teniendo como resultados lo siguiente:

- Los ataques a las empresas y a los usuarios perpetrados por actos criminales de tipo financiero, y por los cuales han sido víctimas, son con el empleo del ransomware, phishing y cryptojacking.
- El 25,10% de ataques de ransomware (secuestro de datos) en el 2017 fueron identificados en nuestro país, la cifra más alta en América Latina, según la empresa de seguridad Eset.
- El cibercrimen también se aprovecha de las vulnerabilidades y, en el Perú, una de las amenazas de este tipo es EternalBlue, que se utilizó para propagar Wannacry en el 2017 y dejó una decena de empresas peruanas perjudicadas y más de 200.000 sistemas afectados en 150 países.
- Otro problema que hace difícil detectar el ransomware, es que el ataque no se ejecuta de forma inmediata. El 47% de las empresas peruanas indican tener poca probabilidad de descubrir en el corto plazo un ataque cibernético sofisticado, según un estudio de EY Perú.
- El 47% de las empresas peruanas indican tener poca probabilidad de descubrir en el corto plazo un ataque cibernético sofisticado, según un estudio de EY Perú.
- Otra mala práctica es no contar con un sistema de backup supervisado. Elba Salas, Gerente General

de INTECNIA, partner exclusivo de Bitdefender en el Perú.

- El caso más conocido en el Perú fue el ciberataque a la naviera del grupo Maersk de Dinamarca. La empresa fue víctima de ransomware de la variante Petya.
- En el Perú hay dos tipos de detecciones de los códigos maliciosos del tipo 'miner', que buscan utilizar la capacidad de procesamiento de los dispositivos de los usuarios para obtener criptomonedas: a través de la modalidad del cryptojacking y el minado directo desde la computadora, laptop u otro equipo.
- A ello se suma otro código malicioso popular en el Perú que es conocida como HoudRat. El RAT (Remote Access Tool) está orientado al control de equipos informático para permitir el acceso remoto del ciberatacante.

En el actual entorno de pandemia, Perú fue afectado por 613 millones de intentos de ciberataque entre enero y junio del 2020. En tanto, en Latinoamérica y el Caribe se elevaron a los 15 mil millones, indica el informe de la plataforma Threat Intelligence Insider Latin America 2020Q2 de Fortinet, que recopila y estudia incidentes de ciberseguridad en todo el mundo. Solo en el último trimestre, las empresas han registrado un aumento considerable en los ataques de "fuerza bruta" o intentos repetidos y sistemáticos para descifrar algoritmos, adivinar credenciales enviando diferentes nombres de usuario y contraseñas débiles de correo electrónico, redes sociales y acceso a Wi-Fi, entre otros. El crecimiento del trabajo remoto y la teleducación ha reavivado el interés de los hackers en los ataques de 'fuerza bruta'. Con la transición masiva a la oficina y el aprendizaje en casa, los ciberdelincuentes encuentran una importante cantidad de servidores de protocolo de escritorio remoto (RDP) mal configurados, lo que facilita este tipo de ataque.

Según datos del estudio titulado Clarity on Cibersecurity (KPMG, 2018), que ha sido elaborado por la consultora internacional KPMG en Suiza, nos señala que el 80% de las juntas de directorios de las organizaciones consideran a la ciberseguridad como una amenaza operativa; sin embargo, solo 36% menciona el tema en sus reportes anuales.

El crecimiento vertiginoso de estos ataques cibernéticos asociados al crimen financiero nos motivó para incluir en este artículo, la evolución de sistemas antifraudes, al respecto en el artículo denominado el impacto de los delitos financieros de Shelley M. Hayes (2020), se afirma:

> Independientemente de la industria, las organizaciones han desarrollado algún componente de programas antifraude. El uso de modelos de aprendizaje de computadoras y los procedimientos analíticos predictivos desarrollados para la detección oportuna de patrones de transacciones y comportamientos atípicos han resultado de gran utilidad (pp.8).

Con el afán de descubrir y prever la criminalidad financiera, muchas organizaciones se esfuerzan en tener una mejor identificación conceptual entre el fraude y el delito financiero.

Con el avance de la tecnología informática y su influencia en casi todas las áreas de la vida social y empresarial, han surgido comportamientos ilícitos llamados de manera genérica delitos informáticos, que han abierto un amplio campo de riesgos y también de estudio e investigación, en disciplinas jurídicas y técnicas, pero especialmente en aquellas asociadas con auditoría de sistemas o auditoría informática (Ojeda & Arias, 2010, pág. 43).

Respecto a los términos de crimen financiero y específicamente en la era cibernética Salim Hasham, Shoan Joshi, y Daniel Mikkelsen (2019) , afirma*: "El crimen financiero generalmente ha significado lavado de dinero y algunas transgresiones de orden criminal, incluyendo el soborno y la evasión fiscal, que involucran el uso de servicios financieros en apoyo de empresas criminales",* asimismo *"El fraude, por otro lado, generalmente designa una serie de delitos, como falsificación, esquemas de crédito y amenazas internas, que implican el engaño del personal o los servicios financieros para cometer un robo"* (pp.2).

En nuestro país, se tiene un mayor uso el concepto de delito financiero que al de crímenes financieros según el título x - delitos contra el orden financiero y monetario del Código Penal (1991), es por ello, que localmente se tiene tipificado dentro de los delitos financieros más comunes, a los robos y la clonación de tarjetas de crédito, cheques falsos, lavado de dinero, fraude. En la actualidad, las líneas divisorias entre el crimen y los delitos financieros están quedando atrás, sobre todo por los insistentes y constantes ataques cibernéticos en estos dos tipos de ilícitos que han sido comentados y definidos, aunado con una dimensión cada vez más sofisticada de estas organizaciones criminales en su actuar delictivo**.**

Según información obtenida de LexisNexis risk solutions (2018) en su artículo: True Cost of Fraud study, nos revela:

> The World Economic Forum señaló que el fraude y los crímenes financieros eran una industria de billones de dólares, informando que las empresas privadas gastaron aproximadamente $ 8,2 mil millones solo en controles contra el lavado de dinero (AML) en 2017. Los delitos en sí mismos, detectados y no detectados, se han vuelto más numerosos y costosos que nunca. En una estimación ampliamente citada, por cada dólar de fraude, las instituciones pierden casi tres dólares, una vez que los costos asociados se agregan a la pérdida por fraude en sí (pp.5).

Según LexisNexis Risk Solutions (2018), esto busca poner en alerta la catastrófica cifra de pérdidas ocasionadas por estas organizaciones criminales, donde nos revela que hay una relación de tres a uno en pérdidas por cada dólar perpetrado criminalmente, dado lo que origina con posterioridad estas estas actividades ilícitas al ser asociados con la totalidad de los costos acarreados con estas actividades criminales. Los crímenes financieros son cada vez más sofisticados a medida que la tecnología se

hace más avanzada, afirmó John Edison, vicepresidente de Productos Cumplimiento y Delitos Financieros en Oracle Financial Services.

Según Shelley M. Hayes (2020), la búsqueda y exploración de la Big Data es posible conseguir los beneficios con el uso de redes más complejas de inteligencia para el análisis de nuevos riesgos, a fin de ponernos a buen recaudo contra los ciberdelincuentes. Los esquemas de la automatización robótica de procesos (Robotic Process Automation, RPA), el aprendizaje de computadoras (machine learning) y la inteligencia artificial (AI, por sus siglas en inglés), son algunas de las opciones que nos ofrece para adoptar nuevas tecnologías desarrolladas (pp.43).

Por ello, el entorno actual requiere fortalecer los controles derivados de los procesos de información que el sector financiero efectúa, como son las transacciones en banca móvil, en consecuencia, conceptos como la ciberseguridad vienen desarrollándose con mucha fuerza en este sector (Ojeda-Contreras, Moreno-Narváez, & Torres-Palacios, 2020; Fuquen, 2014; Joyanes, 2017; Godoy, 2020).

Metodología

La revisión sistemática es una forma de investigación ampliamente aceptado que permite revelar las investigaciones existentes en un área del conocimiento científico (Urra & Barría, 2010) y, se caracterizan por su transparencia y objetividad en el proceso de recolección de la información documental (Moreno, Muñoz, Cuellar, Domancic, & Villanueva, 2018).

La búsqueda se orientó a la automatización inteligente asociada a la detección de los crímenes financieros, en las empresas de servicios financieros, empresas de comercio electrónico, organizaciones gubernamentales y bancos de los países de Estados Unidos y Perú principalmente. En total se encontraron 34.390 casos; de los cuales 14.429 casos corresponden a cyber attack y 20.000 casos a crime finance al gobierno de los Estados Unidos y empresas financieras respectivamente, 209 casos corresponden a cost of fraud en empresas minoristas, comercio electrónico, banca y finanzas respectivamente.

Se realizó una revisión sistemática de las publicaciones. Se elaboró un registro de investigación a partir de la pregunta de investigación: ¿Cómo detectar los crímenes financieros con la influencia de la inteligencia artificial? Para seleccionar los trabajos se definieron como criterios: la inclusión, únicamente, de estudios publicados entre 2016 a 2020, disponibles en texto completo, en ingles español y portugués.

Se ha empleado dos bases de datos: Scopus y LexisNexis para realizar las elecciones de las revistas y artículos.

Textos de la revisión

Teniendo en cuenta que este estudio de revisión tiene como objetivo investigar la influencia de la automatización inteligente en la capacidad para detectar los crímenes financieros. Para ello, hemos considerado algunas variables enfocadas en la automatización artificial y la detección de los crímenes financieros. En nuestra revisión estimamos bajo esta perspectiva apoyarnos en el artículo titulado Financial Crime and Fraud in the Age of Cibersecurity, según Salim Hasham, Shoan Joshi, y Daniel Mikkelsen (2019),donde nos proporciona una mayor referencia cuando comentan las distintas modalidades que se presentan en estos hechos ilícitos.

Se inició la revisión con la exploración de los siguientes buscadores de datos científicos:

Tabla 1. *Resultados de la búsqueda*

Publicaciones	181 casos	**Publicaciones**	Más de 10.000 casos
Clave de búsqueda	Cyber attack	Clave de búsqueda	Crime finance
Frase	Gbno.Federal de U.S.A.	Frase	Gbno.Federal de U.S.A.
Idioma	Inglés	Idioma	Inglés

Fuente: *Elaboración propia en base a LexisNexis Risk Solutions Survey Finds (2018).*
Nota: *Por cada dolar de fraude, las empresas de servicios financieros ahora gastan $ 2,92*

Tabla 2. *Resultados de la búsqueda*

Publicaciones	Más de 10.000 casos	**Publicaciones**	Más de 10.000 casos
Clave de búsqueda	Cyber attack	Clave de búsqueda	Crime finance
Frase	Gbno.Federal de U.S.A.	Frase	Gbno.Federal de U.S.A.
Idioma	Inglés	Idioma	Inglés

Fuente: *Elaboración propia en base a LexisNexis Risk Solutions Survey Finds (2018).*
Nota: *Por cada dólar de fraude, las empresas de servicios financieros ahora gastan $ 2,92*

Tabla 3. *Resultados de la búsqueda*

Publicaciones	72 casos	**Publicaciones**	57 casos
Clave de búsqueda	Cost of fraud	Clave de búsqueda	Banca y Finanzas
Frase	Comercio Electron.	Frase	
Idioma	Inglés	Idioma	Inglés

Fuente: *Elaboración propia en base a LexisNexis Risk Solutions Survey Finds (2018).*
Nota: *Por cada dólar de fraude, las empresas de servicios financieros ahora gastan $ 2,92*

Según LexisNexis Risk Solutions (2018), referente a su publicación denominada True of Cost Study 2020, la investigación nos señala el resultado del aumento de los volúmenes de fraude se traduce en un aumento del 7,3% en el costo del fraude año tras año para el comercio electrónico y los comerciantes minoristas de EE. UU. El multiplicador de fraudes de LexisNexis, la cantidad total de costos relacionados con tarifas, intereses, reemplazo de mercadería y redistribución por dólar de fraude por el cual el comerciante es responsable, muestra que el fraude ahora les cuesta a las empresas $ 3,36 por cada dólar perdido por fraude en comparación con $ 3,13 en 2019 y $ 2,40 en 2016. Este es un aumento de $ 0,96 en cinco años. Los costos de EE.UU son significativamente más altos que el costo que enfrentan los minoristas canadienses por $ 1 perdido por fraude a $ 2,87 (pp.1).

Se da a conocer el hallazgo encontrado, que continúan en ascenso los delitos financieros, donde hasta la fecha de 2020 ha crecido en 7,3% siendo los sectores más afectados, el comercio electrónico y los minoristas.

Tabla 4. *Resultados de la búsqueda*

Publicaciones	72 casos	**Publicaciones**	57 casos
Clave de búsqueda	Cost of fraud	Clave de búsqueda	Cost of fraud
Frase	Prest. Serv. Bancarios	Frase	Payment card service
Idioma	Inglés	Idioma	Inglés

Fuente: *Elaboración propia en base a LexisNexis Risk Solutions Survey Finds (2018).*

Nota: *Por cada dólar de fraude, las empresas de servicios financieros ahora gastan $ 2,92*

Préstamos y Servicios bancarios

El estudio de Lexis Nexis Risk Solutions (2018), sobre su artículo publicado Cost of Fraud Study U.S. Financial Services, nos revela que: Para el sector de servicios financieros, el estudio muestra que, por cada dólar de fraude, las empresas de servicios financieros incurren en costos de $ 2,92 frente a los $ 2,67 en 2017 lo que representa un aumento interanual del 9,3%. El valor perdido de la transacción, más los honorarios e intereses incurridos durante las etapas de solicitud / suscripción / procesamiento, costos laborales para la investigación del fraude, multas y honorarios legales, así como los gastos de recuperación externa son los principales costos del fraude para las instituciones financieras según el estudio (pp.1).

El estudio muestra que las empresas de servicios financieros que son víctimas de fraude, para el periodo 2017 a 2018, tienen un mayor crecimiento de 9,3%, y un mayor gasto de $0,25 en este periodo 2018.

Tabla 5. *Resultados de la búsqueda*

Publicaciones	4.046 casos
Clave de búsqueda	Cyber attack
Frase	Todas
Idioma	Inglés

Fuente: *LexisNexis Cost of fraud, banking, commerce, retail (2020).*

Según, Shamshirbanda y otros (2020) sobre su artículo titulado, Computational intelligence intrusion detection techniques in mobile cloud computing environments: Review, taxonomy, and open research issues, nos confirma:

> Con la creciente utilización de Internet y los servicios que proporciona, se produce un aumento de los ciberataques para explotar la información. Una tecnología para almacenar y mantener la información del usuario que se utiliza principalmente por su simplicidad y servicios de bajo costo es la computación en la nube (pp.1).

Nigrini (2000), nos comenta que la ley Benford ha cumplido un rol clave en los negocios y han contribuido a nuestro bienestar tanto como la rueda, el fuego, y la agricultura. En el campo de la seguridad y auditoría, se usan procedimientos analíticos en base a los números al planear la naturaleza, oportunidad, y alcance de los procedimientos de auditoría y controles.

La ley de Benford, se basa en que una gran variedad de conjuntos de datos numéricos que existen en la vida real, la primera cifra es 1 con mucha más frecuencia que el resto de los números. Esto ha permitido que basado en la lógica de uso de número frecuentes de la ley de Benford y la tecnología se apliquen algoritmos para lograr analizar comportamientos inusuales en una curva de números, utilizando aplicaciones informáticas en el manejo de la base de datos.

Finalmente, la robótica y la inteligencia artificial se complementan, donde la robótica se encarga del diseño, fabricación y empleo de máquinas automáticas programables con el objeto de realizar tareas repetitivas, mientras que la inteligencia artificial apunta a que los robots sean capaces de pensar y tomar decisiones creando una nueva relación muy útil en aplicaciones de ensamblaje robótico. Esta combinación puede generar algoritmos orientados a la detección de crímenes informáticos.

Desarrollo y discusión

Un primer tema para considerar, de las revistas y publicaciones analizados, es de la consultora McKinsey (2018)que expone en forma clara y muy didáctica, las diversas modalidades y/o el nuevo perfil cibernético del fraude y crímenes financieros a través de los ataques de Carbanak.

Resumen de las modalidades de los Ataques Cabarnak

- El spear phishing es una modalidad de estafa a través del correo electrónico o comunicaciones dirigida a personas, organizaciones o empresas específicas.
- Los backdoores son una de las herramientas más utilizadas, de forma maliciosa o no, para acceder a sistemas de usuarios.
- Máquinas infectadas de virus en busca de controlar las computadoras.
- El atacante identificado por la PC observa la pantalla de administración para imitar el comportamiento de administración del sistema de transferencia de efectivo.
- Saldo e importes ficticiamente transferidos.
- Los atacantes programan cajeros automáticos para emitir cómplices de espera de efectivo en un temporizador específico.
- Los atacantes usan pagos en línea y pagos electrónicos a bancos receptores para transferir fondos extraídos.

Los resultados de los robos a los bancos basados en programas de malware ascendieron por un total de más de $ 1 mil millones. Los atacantes, una banda criminal organizada, obtuvieron acceso a los sistemas mediante el fraude o la violación informática consumado mediante correo electrónico denominado phishing y luego transfirieron saldos inflados de manera fraudulenta a sus

propias cuentas o a cajeros automáticos programados para transferirle el efectivo a sus cómplices.

Un segundo tema es, la revisión efectuada dentro del universo de publicaciones de artículos y revistas consultadas, se tiene una publicación muy relevante por parte de la empresa LexisNexis Risk Solutions (2018), el estudio tiene como finalidad brindar una cooperación a las empresas del sector financiero, comerciantes digitales y colocadoras de créditos, donde se muestra hallazgos como:

- El costo promedio del fraude ha crecido en 9,3% para las empresas que brindan servicios financieros, mientras para las empresas que brindan servicios de crédito se incrementó en 8,1% para el año 2017.
- Por cada $1 de fraude perpetrado, le significa un costo de $ 2,92 para las empresas que brindan servicios financieros; $3,05 para las empresas que brindan servicios de crédito y $ 2,56 para las empresas de comercio electrónico.
- Por cada $1 de fraude perpetrado, le significa un costo entre $ 3,00 y $ 3,37 para las empresas grandes y medianas.
- El costo del fraude oscila entre $ 3,26 y $ 3,51 por cada $1 para las empresas que venden productos digitales o realizan operaciones a través el canal móvil.
- Las grandes empresas crediticias y las de servicios financieros, continúan siendo víctimas de estos tipos de fraudes en un 54% y 49% de pérdidas por estos delitos cometidos.

Un tercer tema es**,** dentro de búsqueda de nuestra revisión, nos permitió analizar y tener una mirada local en Perú, teniendo hallazgos importantes en su artículo publicado por la agencia peruana de noticias Andina (Pichihua, S., 2018), relacionados a crímenes financieros perpetrados, e información relacionada al actual entorno de pandemia, donde Perú fue afectado por 613 millones de intentos de ciberataque entre enero y junio del 2020. Un cuarto tema que abordamos es**,** que amerita incluir el artículo publicado por el Peruano (2019) donde destacamos como resultados importantes los siguientes:

- América Latina reporta 46 actos de ataques cibernéticos por día.
- En América Latina, los países más afectados por esta vulnerabilidad son México (23%), Perú (14%) y Brasil (12%).
- La explotación de vulnerabilidades es uno de los métodos más comunes que utilizan los ciberdelincuentes para atacar a sus víctimas. Un estudio de Eset revela que hasta finales del 2018 se registraron 16.555 vulnerabilidades, lo que significa un incremento del 12% respecto al 2017.
- Las principales formas de infección fueron por ejecución de código (23%), error de software por desbordamiento de búfer (18%) y la inyección de scripts (15%), el 79% de las vulnerabilidades de ejecución de código fueron graves.

Conclusiones

- El devenir del desarrollo de las tecnologías de la información y comunicación involucran a varios sectores de nuestra sociedad, entre ellas al sector empresarial. Sin duda la denominada cuarta revolución industrial está en marcha y por lo tanto los procesos de automatización de los trabajos rutinarios de manera inteligente y sistematizada es una necesidad, sin embargo, con la llegada del Covid19 los instintos de supervivencia de las organizaciones han acelerado estos procesos de digitalización. Las empresas han tenido que reinventarse para sobrevivir a este confinamiento social que afecta la liquidez, en ese contexto el uso de las plataformas web, las aplicaciones apps y las redes sociales han permitido que las operaciones sigan realizándose. En ese sentido, por la gran cantidad de datos y sistemas de información que manejan las empresas, se hace necesario fortalecer la ciberseguridad frente a los delitos informáticos que pone en riesgo las operaciones.
- Las estrategias y los controles que se desarrollen contra todo tipo de violaciones informáticas deben estar decididamente alineadas y orientadas con la visión de las empresas de servicios financieros, de entidades colocadoras de créditos y las de comercio (minoristas y en línea / móviles) para hacer frente a los crímenes financieros, y no emplear estrategias no vinculantes o no asociada a su plan de negocios.
- Las investigaciones de LexisNexis Risk Solutions (2018), ponen de relieve que los ataques de crímenes financieros continúan en una escalada creciente, con deterioros relevantes en las empresas medianas y grandes. Sin embargo, también se extiende para las pequeñas empresas, pero el mayor peso promedio de violaciones de estos cibercrímenes financieros es para las medianas y grandes empresas.
- De nuestra revisión de la información analizada, las unidades de negocios necesitan en forma constante contar con los servicios de una efectiva reingeniería y controles en sus procesos para incrementar la eficiencia en el uso de los bienes con los que tienen a bien disponer y así encaminarse hacia un plan holístico y competente de prevención, detección y dar mayores garantías eficaces contra los crímenes cibernéticos de índole financiero.
- Las investigaciones de Mc Kinsey & Company (2018), ponen en manifiesto que se hace imperiosa la necesidad que las empresas, víctimas de estos ataques financieros se integren en sus experiencias en su lucha contra el crimen cibernético de índole financiero, siendo una decisión que se debe tomar, dado que los perpetradores de estos actos criminales sus actividades se conjugan con sus cómplices que son especialistas en cometer estos delitos.
- Entre los temas más destacados corresponde mencionar que se ha desarrollado, por parte de la consultora McKinsey, un cuadro de riesgos que van a ayudar a poder identificar a los clientes, hacer un seguimiento y detectar irregularidades que alerten

sobre operaciones y comportamientos sospechosos para atenuar en ser víctimas de delitos financieros como los son: los crímenes financieros, fraude, Ciberseguridad, entre otros delitos financieros.

- Organizaciones como NIST en Estados Unidos vienen desarrollando normativas que buscan alinearse a la implementación de controles que protejan a la empresa de ataques cibernéticos, y apoyen el objetivo estratégico de incrementar la calidad y eficiencia operacional" en materia de seguridad.

Referencias

Abaimov, S., & Martellini, M. (2017). *Cyber arms, security in cyberspace.* Estados Unidos: CRC Press.

Arcenegui-Rodrigo, J., Obrero-Castilla, V., & Martín-Lozano, J. (2016). Propuesta de un modelo para la prevención y gestión del riesgo de fraude interno por banca paralela en los bancos españoles. *Cuadernos De Contabilidad, 16*(42), 625-660. doi:https://doi.org/10.11144/Javeriana.cc16-42.pmpg

Arocena, G. (2012). La regulación de los delitos informaticos en el código penal argentino. *Boletín Mexicano de Derecho Comparado, XLV*(135), 945-988. Recuperado el 12 de Mayo de 2021, de https://www.redalyc.org/pdf/427/42724584002.pdf

Bilbao, A., García, B., & Rios, Y. (2009). *El fraude contable: Un enemigo que convive con las Pymes.* Trabajos De Grado Contaduría UdeA, Universidad de Antioquia. Obtenido de https://revistas.udea.edu.co/index.php/tgcontaduria/article/view/323584

CIBERElcano. (2017). *Informe mensual de ciberseguridad.* Madrid: Fundación Real Instituto Elcano de Estudios Internacionales y Estratégicos-THIBER.

Código penal. (1991). Decreto legislativo 635. Poder ejecutivo. Perú. Obtenido de http://spij.minjus.gob.pe/content/publicaciones_oficiales/img/CODIGOPENAL.pdf

El Peruano. (14 de Enero de 2019). Ciberataques en crecimiento. *El Peruano*. Obtenido de https://elperuano.pe/noticia/74748-ciberataques-en-crecimiento

Fuquen, H. (2014). Ciberseguridad en el sector bancario. Una aproximación a la innovación en el sector financiero . *Desarrollo tecnológico e innovación empresarial, 1*(3), 15-18. Obtenido de https://www.colinnovacion.com/wp-content/uploads/Articulo-3-Edicion-3-Volumen-1.pdf

Godoy, J. (2020). Bancarización, digitalización y banca móvil. Evolución de los modelos de negocios bancarios, en la economía digital de Panamá. *Revista FAECO Sapiens , 3*(2), 13-37. doi:https://www.revistas.up.ac.pa/index.php/faeco_sapiens/article/view/1362/1119

González, L., & Lemus, S. (2017). *Robotic Process Automation (RPA).* (C. Insights, Ed.) España: Deloitte .

Guerrero, B., & Castillo, D. (2017). *Desafíos técnicos y jurídicos frente al ciberdelito en el sector bancario colombiano.* Trabajo de grado, Universidad Nacional Abierta y a DIstancia , Escuela de ciencias básicas tecnología e ingeniería , Bogotá. Obtenido de https://repository.unad.edu.co/bitstream/handle/10596/13387/52498805.pdf?sequence=5&isAllowed=y

Hasham, S., Shoan, J., & Mikkelsen, D. (2019). *Financial Crime and Fraud in The Age Cybersecurity.* McKinsey & Company.

Hayes, S. M. (2020). *El impacto de los delitos financieros.* México : KPMG. Obtenido de https://assets.kpmg/content/dam/kpmg/mx/pdf/2020/06/El-impacto-de-los-delitos-financieros.pdf

Ibarra-Mares, A., & Echeverri-Gutiérrez, C. (2018). *Hacia una taxonomía para analizar el crimen económico.* Medellín: Sello Editorial Coruniamericana.

Joyanes, L. (2017). la colaboración público-privada en la era de la cuarta revolución industrial (Industria 4.0 versus ciberseguridad 4.0). *Cuadernos de estrategia, 185*, 19-64. Obtenido de https://dialnet.unirioja.es/ejemplar/468096

KPMG. (2018). *https://home.kpmg.* Obtenido de Claridad sobre la seguridad cibernética: https://home.kpmg/ch/en/home/insights/2018/05/clarity-on-cyber-security.html

KPMG. (2020). *Temas claves de ciberseguridad en la nueva realidad.*

LexisNexis Risk Solutions. (2018). *True cost of fraud study.* Obtenido de https://advance.lexis.com/api/document?collection=news&id=urn:contentItem:5TFB-3961-JB72-10

McKinsey & Company. (2018). *Transforming Risk Management with Advanced Analytics.*

Moreno, B., Muñoz, M., Cuellar, J., Domancic, S., & Villanueva, J. (2018). Revisiones Sistemáticas: definición y nociones básicas. *Revista clínica periodoncia, implantología y rehabilitación oral, 11*(3), 184-186. doi:10.4067/S0719-01072018000300184

Nigrini, M. J. (2000). *Digital Analysis Using Benford's Law: Tests & Statistics for Auditors.* Global Audit Publications.

NIST. (2014). *Framework for Improving Critical Infrastructure Cybersecurity.* Obtenido de NIST. Versión 1.0: www.nist.gov/cyberframework

Ojeda, J., & Arias, M. (2010). Delitos informáticos y entorno jurídico vigente en Colombia. *Cuadernos Contables, XI*(28), 41-66. Recuperado el 5 de Mayo de 2021, de

http://www.scielo.org.co/pdf/cuco/v11n28/v11n28a03.pdf

Ojeda-Contreras, F. I., Moreno-Narváez, V. P., & Torres-Palacios, M. M. (2020). Gestión del riesgo y la ciberseguridad en el sector financiero popular y solidario del Ecuador. *CIENCIAMATRIA Revista Interdisciplinaria de Humanidades, Educación, Ciencia y Tecnología, 6*(2), 192-219. doi:DOI 10.35381/cm.v6i2.366

Organización de los Estados Americanos. (2019). *Desafíos del riesgo cibernético en el sector financiero para Colombia y America Latina.* Recuperado el 21 de Mayo de 2021, de https://www.oas.org/es/sms/cicte/docs/Desafios-del-riesgo-cibernetico-en-el-sector-financiero-para-Colombia-y-America-Latina.pdf

Paytán, P. (1 de Marzo de 2019). Ciberataques se disparan. *Semana económica*. Obtenido de https://semanaeconomica.com/management/digitalizacion/331812-ciberataques-se-disparan

Pichihua, S. (2018). ¿Cuáles son los ciberataques más comunes en el Perú? *Andina*. Obtenido de https://portal.andina.pe/edpespeciales/2018/ciberataques-peru/index.html

Shamshirbanda, S., Fathi, M., Chronopoulos, A., Montieri, A., Palumbo, F., & Pescapè, A. (2020). Computational intelligence intrusion detection techniques in mobile cloud computing environments: Review, taxonomy, and open research issues. *Journal of Information Security and Applications, 55*. doi:https://doi.org/10.1016/j.jisa.2020.102582

Singh, A. &. (2019). An Empirical Study of AML Approach for Credit Card Fraud Detection-Financial Transactions International . *Journal of Computers, Communications&Control, 14*(6), 670–690. doi:https://doi.org/10.15837/ijccc.2019.6.3498

Urra, E., & Barría, R. (2010). La revisión sistematica y su relación con la práctica basada en la evidencia en salud. *Revista Latino-America Enfermagem*, 1-8. Recuperado el 12 de Octubre de 2020, de https://www.scielo.br/pdf/rlae/v18n4/es_23.pdf