Derecho informático: la necesidad de una reforma en la política pública del MICITT ante el incremento de los delitos cibernéticos en Costa Rica, producto de la pandemia del Covid-19

María Vanessa Zamora González[1]*, Universidad Latinoamericana de Ciencia y Tecnología*

2021

1. Introducción

El desarrollo explosivo de las tecnologías de la información y la comunicación (TIC), referidas fundamentalmente a la informática (uso de las computadoras) y las telecomunicaciones (Internet) ha modificado radicalmente el quehacer humano y transformado los patrones de comportamiento y las relaciones sociales. Los beneficios que las TIC aportan a la sociedad actual son diversos y evidentes. Sin embargo, el amplio desarrollo de estas tecnologías ofrece también un aspecto negativo: ha abierto la puerta a conductas antisociales y delictivas que se manifiestan de formas que hasta ahora no era posible imaginar. (PROSIC, 2010)

Así, el crecimiento de las transacciones digitales en el mundo, el impulso de la bancarización a través de medios digitales y la crisis sanitaria producto de la pandemia del COVID-19, han hecho que el fraude bancario se haya promovido también a ritmos exponenciales, pasando de ser un fenómeno que afectaba transacciones físicas en su mayoría, y muy pocas en medios digitales o de internet, a afectar predominantemente transacciones digitales y un porcentaje mucho menor en transacciones físicas.

En este sentido, los estafadores están aprovechando nuevas tecnologías y recursos para generar estafas y fraudes sofisticados y creativos hacia los clientes bancarios, los bancos, comercios y grandes cadenas que utilizan los datos de los clientes.

Los delitos informáticos, el fraude, el cibercrimen, y otros; han sido un tema que ha cambiado conforme ha evolucionado la tecnología, y su impacto en Latinoamérica ha sido fuerte debido a que mucho del fraude que sucede en Europa y Norteamérica, posteriormente migra hacia Latinoamérica, esto debido a que lamentablemente las tecnologías para medios de pago, ingresan en algunos casos más tarde que en estas zonas geográficas. (Rodríguez, 2020)

[1] Estudiante de Licenciatura en Derecho, educarse2019@gmail.com

Desde el 2017 se percibió en el sector financiero costarricense un aumento en los indicadores de fraude transaccional, específicamente en las transacciones realizadas por los clientes a través de internet, lo cual afecta una parte importante de ellos; en ocasiones a los mismos comercios, y a las instituciones financieras que ofrecen los productos. Dicho incremento se percibió en toda la región de Latinoamérica y se dieron casos importantes en Norteamérica que afectaron a nuestra región. (Rodríguez, 2020)

A raíz de lo anterior, y como lo señala KPMG en una encuesta global de fraude bancario del 2019 (KPMG, 2019), se desarrollan nuevas tipologías de fraude que empiezan a sorprender a los usuarios y a los bancos, quienes tienen que agilizar la identificación de las causas o razones que originan que estas tengan éxito, para empezar a cerrar estas brechas en tiempo récord.

En los últimos tres años, se ha generado un incremento del fraude bancario en algunos países de la Región Latinoamericana, sobre todo en las transacciones que realizan los clientes por internet, lo que genera preocupación en los clientes y en los comercios; además de pérdidas y desconfianza en los productos bancarios. El incremento del comercio por internet, sobre todo por fenómenos externos como la pandemia mundial del COVID 19, ha propiciado el aumento, casi de forma paralela, de los fraudes en los productos bancarios en línea. (Rodríguez, 2020)

En Costa Rica, la seguridad informática, aunque aparece con bastante frecuencia en la cotidianidad de las personas y las organizaciones que enfrentan situaciones concretas de ataques informáticos, no ha sido abordada de manera integral, ni ha constituido materia de atención explícita por parte de una población y de una institucionalidad que cada vez con mayor frecuencia e intensidad emplea las tecnologías de la información y la comunicación. En general, la ciberseguridad se circunscribe a la esfera de los expertos y no se ha avanzado lo suficiente en el desarrollo de una cultura colectiva en este campo. (PROSIC, 2010)

Esto quiere decir que el fraude cambia de acuerdo con el entorno de los sistemas de pagos. Por lo tanto, en este artículo académico se investigará los aspectos relacionados con el derecho informático y se buscará exponer la necesidad de una reforma en la política pública ante el incremento de los delitos cibernéticos en Costa Rica, producto de la pandemia del Covid-19. Se procederá a determinar cómo ha evolucionado el fraude, cuál es su estado actual, cuáles son esas

nuevas tipologías que han proliferado a partir de la incursión masiva de la virtualización de las transacciones bancarias y comerciales producto de la crisis sanitaria, y de qué manera se pueden identificar sus razones, para así poder gestionarlas o mitigarlas.

Por lo anteriormente planteado, surge la siguiente pregunta de investigación o interrogante principal: ¿qué tipo de reforma a nivel de política pública se debería generar en la institucionalidad pública, a partir del MICITT y otros entes actores, ante el incremento de los delitos cibernéticos en Costa Rica, producto de la pandemia del Covid-19?

2. Revisión bibliográfica

A la hora de pensar en la ciberseguridad, el problema no radica en el progreso tecnológico; sino en cómo se va a utilizar esa tecnología; y más importante, quién y cómo se va a regular. Es fácil pensar en los beneficios que puede conseguir una cierta máquina; pero si no se piensa en los perjuicios que puede acarrear, su futuro será dañino para la sociedad. Un burdo y claro ejemplo es la creación de internet. Se crea con la idea de poder conectar a miles de personas de todo el mundo por muy lejos que estuvieran (beneficio), pero no se pensó en qué necesidades de seguridad iba a requerir; por ejemplo, para que no se pudiera entrar en nuestro ordenador, encriptar todos nuestros archivos y pedir dinero por ellos (perjuicio). (Nieto, 2019)

La tecnología y su consideración como tema tabú, a pesar de estar en pleno siglo XXI, se da a causa de los perjuicios que pueden provocar ciertas tecnologías que han salido al mercado sin tener en cuenta todas sus variables de seguridad, acceso y prevención; que se hayan sacado a la venta antes de tiempo porque otra compañía hace la competencia y por ese motivo no se han detenido a pensar si su objeto es seguro y si la información está debidamente resguardada frente a terceros o por un uso inadecuado o no autorizado.

Un especialista en derecho cuenta con un conocimiento sobre el delito desde la visión de muchas disciplinas distintas (medicina, psicología, derecho informático, criminología, sociología), lo cual lo convierte en un profesional fundamental e imprescindible en un equipo de ciberseguridad para prevenir tanto que cualquier avance tecnológico se pueda convertir en un *hotspot* para

ciberdelincuentes, como que un determinado grupo de personas se conviertan en un *target* para estos delincuentes, es decir, ciber víctimas. (Nieto, 2019)

En este sentido, se debe comprender que la ciberseguridad no se trata únicamente de los ceros y unos dentro del ordenador. El eslabón más vulnerable en esta cadena de seguridad es el usuario. En la ciberseguridad hay que tener en cuenta muchos aspectos; no dejar contraseñas en un *post – it* sobre el escritorio; asegurarse de estar protegidos mediante antivirus, tener un ordenador actualizado y libre de vulnerabilidades, cerrar las sesiones cuando se sale de un ordenador, crear contraseñas seguras (no 1234 o similares), entre otros. Como se observa, el factor humano afecta a la ciberseguridad de una manera enorme. No se debe olvidar que el ordenador hará lo que nosotros queramos que haga. (Nieto, 2019)

Han surgido nuevas maneras de atentar contra la privacidad y el patrimonio de las personas y las empresas, y para cometer delitos de tipo tradicional en formas no tradicionales. Los llamados delitos informáticos, que constituyen actos delictivos que se cometen con la ayuda de las TIC, aumentan los riesgos en el ciberespacio y ponen en entredicho la seguridad informática, se han ido multiplicando en los últimos años de manera exponencial. Son numerosas las formas y los ámbitos en que se presentan los ciberdelitos. (PROSIC, 2010)

Como ejemplos de lo anterior, se tienen nuevos tipos de fraudes en tarjetas, fraudes y estafas en las plataformas de banca en línea de las instituciones, fraudes por robos de identidad, ataques de fuerza bruta, fraudes por tomar el control de cuentas o grupos de cuentas de un emisor de tarjetas, compromisos de datos, y otros. Al mismo tiempo, las instituciones bancarias deben trabajar con mejores tecnologías de detección y monitoreo, con modelos matemáticos y perfilamiento, para poder llevar un balance entre contrarrestar el fraude, y el permitir a sus clientes transaccionar de forma segura en internet utilizando sus plataformas.

En términos generales, se reconocen cuatro grandes categorías: fraudes cometidos mediante la manipulación de computadoras, las falsificaciones informáticas, las modificaciones de programas o datos computarizados, y el acceso no autorizado a servicios y sistemas informáticos. A manera de ilustración pueden citarse los siguientes delitos informáticos: violación de la privacidad, divulgación de material ilegal, sustracción de datos, modificación de los programas existentes o

inserción de nuevos programas o rutinas (virus y gusanos), fraude bancario, espionaje informático e incluso ataques de naturaleza militar a las plataformas informáticas de un país (ciberguerra), entre otros. Desde el punto de vista tecnológico, la aparición de aplicaciones cada vez más complejas y costosas para la protección de equipos y redes disminuye el riesgo, pero no garantiza inmunidad total. (PROSIC, 2010)

Tipos de fraudes

Como parte del desarrollo de la investigación, es necesario introducirse en los tipos de fraude actuales, y comunes que se están generando en los ámbitos de comercio electrónico y la banca electrónica; motivo por el cual se deben subdividir en dos grupos; es decir, los que suceden por medio de tarjetas de crédito en el mundo de tarjeta no presente, y los que suceden en el mundo de la banca electrónica.

Fraude realizado por medio de Tarjetas

1) *Carding* o *credit master*: es una modalidad de fraude electrónico en el cual las personas detectan cargos no reconocidos en sus tarjetas de crédito o de débito. Los delincuentes acceden de forma ilegal, a través de un software, de manera aleatoria, a la información de tarjetas de crédito o débito. Una vez que obtienen la información, realizan pagos con ellas, que, en primera instancia, pueden pasar desapercibidos, ya que son montos muy poco significativos, por lo que son detectados en el momento en el que los tarjetahabientes perciben cargos que desconocen.

2) *Account Take Over* (ATO): en español es adquisición de la cuenta. De acuerdo con Castañeda (2020)

> El ATO (account take over) tiene por objetivo hacerse con el control de la cuenta de la banca online de cualquier usuario. Para conseguirlo despliega toda una serie de tácticas tan conocidas como el phishing, malware, llamadas telefónicas fraudulentas, keylogger, etc. En ocasiones, es posible incluso que la víctima no sea consciente de que ha sido comprometida, porque ha sido infectada sin darse cuenta, como sería por ejemplo el caso de los troyanos de acceso remoto.

3) Fraude en tarjeta no presente. Según Inversiopedia (2020)

> El fraude de tarjeta no presente es un tipo de estafa de tarjeta de crédito en la que el cliente no presenta, físicamente, la tarjeta al comerciante, durante la transacción fraudulenta. El fraude de tarjeta no presente puede ocurrir con transacciones que se llevan a cabo en línea o por teléfono. Teóricamente, es más difícil de prevenir que el fraude presente en la tarjeta, porque el comerciante no puede examinar, personalmente, la tarjeta de crédito en busca de signos de posible fraude, como la falta de un holograma o un número de cuenta alterado.
>
> Los procesadores de pagos con tarjeta de crédito toman una serie de medidas para minimizar el fraude de tarjeta no presente. Estos incluyen la verificación de que la dirección proporcionada por el cliente, en el momento de la compra, coincide con la dirección de facturación en los archivos de la compañía de la tarjeta de crédito, la verificación de la validez de los códigos de seguridad CVV de tres dígitos y la prohibición de los comerciantes de almacenar estos códigos. Sin embargo, si el delincuente ha robado estos datos, la transacción fraudulenta puede parecer legítima.

4) Robo o pérdida: este tipo de fraude es uno de los más antiguos y es donde el estafador toma ventaja del tiempo, en el que el cliente no se ha percatado de que perdió o extravió la tarjeta, y le realizan transacciones fraudulentas a su nombre en este lapso.

5) *Friendly Fraud*: el fraude amistoso consiste, de acuerdo con Riquelme (2017), en

> El fraude amistoso (friendly fraud) ocurre cuando una persona que sí realizó un cargo a su tarjeta de crédito o débito no lo reconoce y exige que su dinero le sea devuelto. También existen casos en los que un consumidor adquiere un producto vía Internet y aunque éste sí es entregado en el domicilio indicado, el comprador reclama que no fue entregado o que lo devolvió. Estos fraudes afectan al 42 % de los comerciantes, que realizan ventas tanto de productos físicos como de bienes digitales, los cuales son llamados comerciantes híbridos.

En este tipo de fraude, Posner (2019) indica lo siguiente

> Un comprador en línea hace una compra y luego mete un contracargo alegando que la tarjeta fue robada. El contracargo suele presentarse después de que los bienes ya fueron entregados. Este tipo de fraude suele hacerse por consumidores que saben muy bien lo que están haciendo, y suele ser difícil de detectarse, porque los bancos suelen favorecer a sus clientes en el tema de los contracargos.

6) Fraude en comercios afiliados: el fraude en comercios afiliados se presenta cuando el mismo comercio se presta para la utilización de sus plataformas para transaccionar con tarjetas robadas, o en el caso del e-commerce, utilizar su plataforma para que se transaccione con datos de tarjeta recolectados de forma fraudulenta. También, este tipo de fraude se da cuando el comercio recibe pruebas y, posteriormente, transacciones en sus plataformas, y por falta de seguridad del comercio en sus páginas, debe asumir el costo de dichos fraudes. (Rocha, 2020)

El segundo grupo es el fraude realizado mediante la banca en línea o banca electrónica

1) Phishing. En Malware Bytes (2020) se indica lo siguiente

> Phishing es el delito de engañar a las personas para que compartan información confidencial como contraseñas y números de tarjetas de crédito. Como ocurre en la pesca, existe más de una forma de atrapar a una víctima, pero hay una táctica de phishing que es la más común. Las víctimas reciben un mensaje de correo electrónico o un mensaje de texto que imita (o "suplanta su identidad") a una persona u organización de confianza, como un compañero de trabajo, un banco o una oficina gubernamental. Cuando la víctima abre el correo electrónico o el mensaje de texto, encuentra un mensaje pensado para asustarle, con la intención de debilitar su buen juicio al infundirle miedo. El mensaje exige que la víctima vaya a un sitio web y actúe de inmediato o tendrá que afrontar alguna consecuencia.
>
> Si un usuario pica el anzuelo y hace clic en el enlace, se le envía a un sitio web que es una imitación del legítimo. A partir de aquí, se le pide que se registre con sus credenciales de nombre de usuario y contraseña. Si es lo, suficientemente ingenuo, y lo hace, la información de inicio de sesión llega al atacante, que la utiliza para

robar identidades, saquear cuentas bancarias, y vender información personal en el mercado negro.

2) Ingeniería social: en el contexto de esta investigación, esta modalidad de estafa es explotada para el fraude bancario en plataformas de banca en línea. Interpol (s.f.) indica

> El fraude basado en la ingeniería social abarca a todos los métodos utilizados por los delincuentes para explotar la confianza de una persona, con el fin de obtener dinero, directamente o información confidencial, que les permita realizar un delito posterior. Los medios sociales son el canal preferido para ello, aunque no es inusual que el contacto se realice por teléfono o en persona.

La ingeniería social es una de las formas más comunes para cometer un fraude en las plataformas de banca en línea.

Actores que intervienen en las transacciones bancarias

En la figura 1 se muestra de manera gráfica, cuáles son los actores que intervienen en las transacciones bancarias, en las cuales se genera el riesgo de fraude.

Figura 1. Actores que intervienen en los servicios y productos bancarios. Recuperado de: Rodríguez, 2020.

Como se observa en la figura anterior, los actores son: a) cliente, b) comercios, c) bancos, d) E-commerce. Los procesadores, muchas veces, son un outsourcing de los bancos u operan como un banco. Dado que todos los actores que participan en las transacciones bancarias giran en torno al riesgo de fraude, surge la pregunta: ¿cuáles son los causantes de dichos incrementos?

Brechas relacionadas con ataques de fraude

Como parte de los conceptos que se incluyen en este capítulo, se menciona de forma general, las brechas que más afectan a las empresas hoy en día; es decir, las debilidades en el ámbito de la seguridad, que pueden permitir casos de robo de información y que, a la postre, facilitan el robo de datos de una empresa; o los compromisos de información, que perjudican, fuertemente, a los bancos hoy en día, debido a debilidades en sus aplicaciones o sus desarrollos.

Una brecha tiene que ver con una falla en los sistemas, o en los procedimientos que ocasionan que las instituciones financieras, y en muchos casos, los comercios, comprometan los datos personales de sus clientes. Estas brechas permiten que los estafadores ingresen y se apropien de esta información, y la utilicen para comerciarla o usarla directamente en la elaboración del fraude.

Las brechas de seguridad son incidentes que afectan, principalmente, datos de carácter personal, sensibles para la persona o para la organización. De acuerdo con la Agencia Española de Protección de Datos (2019), la brecha de seguridad se define como:

> Una brecha de seguridad es un incidente de seguridad, que afecta a datos de carácter personal. Este incidente puede tener un origen accidental o intencionado y además puede afectar datos tratados, digitalmente, o en formato de papel. En general, se trata de un suceso, que ocasione destrucción, pérdida, alteración.

Después de dar un repaso muy general a este problema y establecer que definitivamente facilita que el fraude opere con datos que recolectan en los incidentes y que los estafadores compran y utilizan en ataques secuenciales u otros tipos de fraude, se procede a ver los tipos de brechas como una referencia más detallada de este fenómeno. Para hablar de las principales brechas, se puede referenciar OWASP que, como indica Rivera (2020) en su blog

> Según OWASP, este es el top 10 de principales riesgos de seguridad en aplicaciones web:

a) Injection (inyección).

b) Broken Authentication (autenticación vulnerada).

c) Sensitive Data Exposure (exposición de data sensible).

d) XML External Entities (XXE) (XML entidades externas).

e) Broken Access Control (control de acceso vulnerado).

f) Security Misconfiguration (falta de configuración de seguridad).

g) Cross-Site Scripting (XSS), (secuencia de comandos en sitios cruzados).

h) Insecure Deserialization (ataque con data o usuario no conocido).

i) Using Known Vulnerable Components (uso de componentes vulnerables no conocidos).

j) Insufficient Logging & Monitoring (monitoreo insuficiente).

El tema de las vulnerabilidades es importante mencionarlo en este estudio, debido a que es parte de las razones de la proliferación del fraude en las transacciones que se dan a través de Internet, es decir, por el comercio electrónico. Las brechas de seguridad abren una posibilidad para el robo de información. En el estudio elaborado por KPMG (2019) llamado Encuesta global de fraude bancario, se mencionan algunos de los casos más importantes de robo de información en empresas que mantenían muchos datos de clientes y, en algunos de ellos, lograron robar no solo datos de clientes, sino también datos completos de tarjetas de crédito. En la figura 2 se muestran ejemplos de este tipo de compromisos de información.

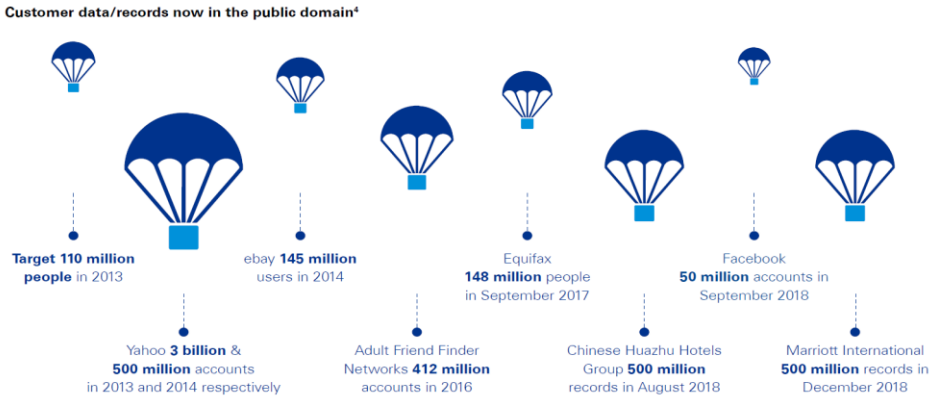


Figura No. 2. Tipo de compromisos de la información. Recuperado de KPMG, 2019

Los estudios formales son escasos en este tema, al menos en América Latina; sin embargo, se puede citar la tesis de grado de Acevedo y Alvarado (Acevedo, 2013) titulada *Migración de banda magnética a chip para evitar fraudes de clonación de tarjetas de crédito o débito. ¿Los bancos ecuatorianos están preparados para este cambio?*, que señala muchos de los tipos de fraude que afrontaba un país de Latinoamérica. Se investigaba si los bancos estarían preparados para la migración de la banda a magnética a chip, que se creía en ese momento estaría minimizando los niveles de fraude que se daban en ese momento por la clonación de banda magnética.

Brechas legales

El sistema jurídico casi siempre va un paso atrás en cuanto a la creación de un marco normativo que permita sancionar a los hackers y a los piratas informáticos. La identificación y captura de las personas y organizaciones criminales que han hecho un negocio del robo de identidades, los fraudes virtuales y las agresiones infecciosas, conllevan dificultades inherentes y demandan especialización y gran cantidad de recursos represivos A estas dificultades, debe agregarse el hecho de que los ciberdelitos son por lo general de naturaleza global; es decir, ocurren en ámbitos que transcienden las competencias nacionales. (PROSIC, 2010)

Así lo reconoce el Programa de Acción de Túnez para la Sociedad de la Información (2019) en el que se destaca: “la importancia de luchar contra el cibercrimen, incluido aquél cometido en una jurisdicción pero que repercute en otra.” También se enfatiza: “la necesidad de concebir instrumentos eficaces y mecanismos eficientes, a nivel nacional e internacional, para promover la cooperación internacional entre los organismos encargados de aplicar la ley en materia de ciberdelito.” Este conjunto de elementos y circunstancias ponen en evidencia que enfrentar las amenazas informáticas no es una tarea fácil. En verdad se requiere de una cultura de la ciberseguridad, cuyos rasgos principales deben incluir: la sensibilización sobre el problema, la responsabilidad, la respuesta oportuna, el respeto a los intereses legítimos, la adhesión a los valores democráticos, la estimación de los riesgos, la implementación de los instrumentos de protección, la gestión de la seguridad, y la evaluación continua (Resolución 57/239 de la ONU).

3. Metodología

La presente investigación es de tipo descriptiva, exploratoria, con un enfoque cuantitativo donde primero se realizará una revisión bibliográfica para conocer los antecedentes y la evolución del tema del derecho informático, los delitos cibernéticos y las políticas públicas en materia del combate al cibercrimen a nivel nacional.

En cuanto al carácter, el fraude, su incremento y sus razones, es un tema poco estudiado, por lo que se ajusta a una investigación exploratoria, pues las fuentes existentes obedecen a estudios recientes e investigaciones por parte de medios de prensa, industria bancaria, tesis, estándares internacionales de protección de datos, que tratan de indagar sobre el tema del fraude y su incremento, las cuales son relativamente fuentes recientes, así como la ausencia de información, noticias, jurisprudencia e información legal que respalde estos planteamientos.

Asimismo, se aplicó un cuestionario de 6 preguntas (técnica de recolección de datos a través de Google Forms) a un grupo de personas especialistas en el tema de derecho informático, delitos cibernéticos, políticas públicas, y subsecuentemente también se incluyeron en la muestra, personas conocedoras o especialistas a nivel nacional en el ámbito de las políticas públicas en materia de derecho informático ante el incremento de los delitos cibernéticos en Costa Rica. Por las razones anteriormente indicadas, se considera la utilización del tipo de muestreo por juicio de expertos.

Fuentes de información

a. Primarias: cuestionario a ocho expertos en la administración de fraude, residentes en Costa Rica, que cuentan con suficiente experiencia y que trabajan día a día administrando en una entidad financiera este fenómeno. Se pretende extraer información de primera mano, tanto del origen de su incremento como de las brechas que intervienen en el proceso y que facilitan el fraude. Con esto, se desea tener como fuente primaria de información la verdad de lo que sucede en Costa Rica por encima de los estudios, investigaciones, y demás, que se logre recolectar.
b. Secundarias: se exploran reportajes, foros, investigaciones serias del fenómeno del fraude como una fuente secundaria, debido a que proporciona un complemento muy importante para confirmar o contradecir la posición de los expertos entrevistados.

Para efectos de este estudio, también forma parte de la investigación, toda la información disponible acerca de registros, artículos, estudios relacionados con temas de fraude, cuestionarios aplicados a profesionales en la administración de fraude (residentes en Costa Rica), sobre este fenómeno en los últimos años, con el fin de conocer su opinión sobre el estado, incremento y razones del fraude bancario en algunos países de Latinoamérica.

En el caso del presente estudio, se utiliza una muestra no probabilística, seleccionada de acuerdo con las publicaciones, estudios, y estadísticas que describen el fenómeno estudiado, a criterio del autor, además de aplicar una entrevista dirigida a un grupo de profesionales en la gestión del riesgo de fraude bancario.

Una vez que se obtiene la información, tanto a través del análisis documental como la generada a partir de la encuesta aplicada, se procede a realizar un análisis de los datos, los cuales contribuyen con elementos e insumos que propician una serie de reflexiones tendientes al desarrollo de los objetivos específicos y la pregunta de investigación. Al mismo tiempo permiten construir una serie de conclusiones y recomendaciones para la política pública a nivel de derecho informático y delincuencia cibernética en nuestro país.

Aplicados los instrumentos a los sujetos y fuentes de información, los tipos de fraude y los actores en el proceso del fraude, se realiza una comparación entre los resultados, y se consideran las respuestas y reflexiones como base para la elaboración de las conclusiones.

4. Resultados

De acuerdo con un estudio del periódico La Nación (Artavia, 2020), denominado *Pandemia Covid-19 dispara las ciberestafas* se muestra cómo se han incrementado las estafas entre el 2019 y 2020.

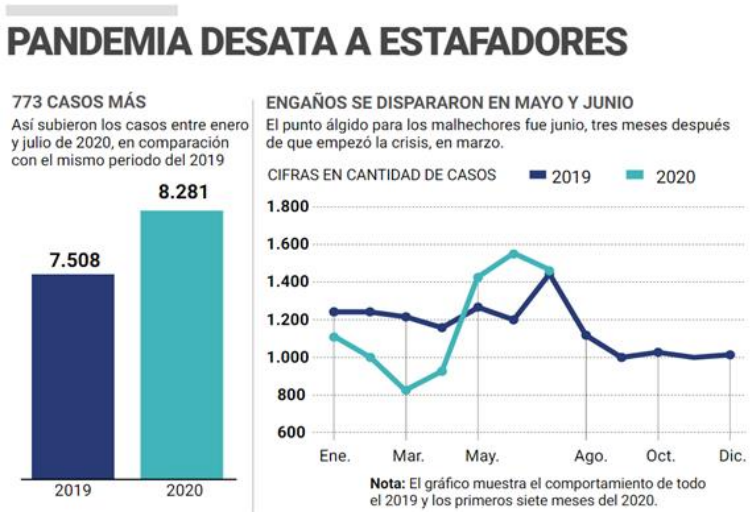


Figura No 3. Incremento de casos de estafas en Costa Rica de acuerdo con la Policía Judicial. Recuperado de Artavia, 2020

En este estudio se puede observar cómo está aumentando el nivel de denuncias por estafas en periodo de pandemia, en donde se busca obtener las credenciales de los clientes para trasladar dinero a cuentas de las organizaciones criminales mediante algún tipo de engaño. En cuanto a la suplantación de identidad, el mismo estudio muestra lo siguiente

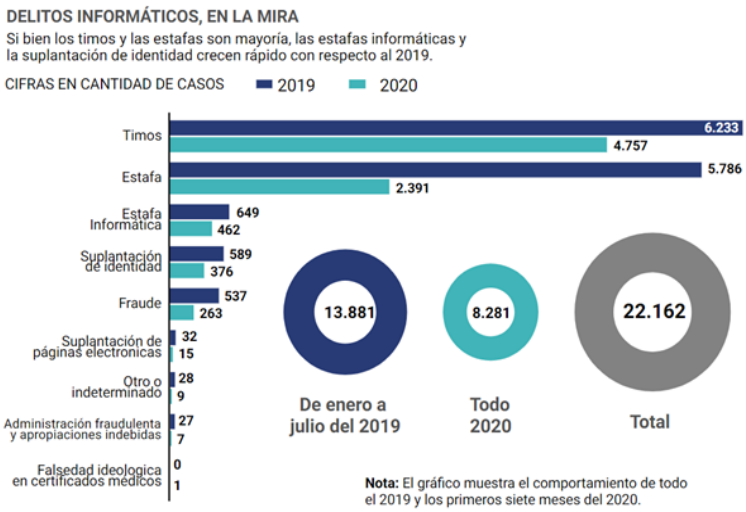


Figura No 4. Crecimiento de suplantación de identidad en el 2020. Recuperado de Artavia, 2020

En cuanto al campo nacional, Salas (2019) en su artículo publicado en La Nación sobre el incremento de las estafas y fraudes por internet, titulado *"Ticos sufrieron 55.000 estafas por*

Internet en un año, según estimación de INEC" expone estadísticas del crecimiento de un 242% en estafas con respecto al 2014, y pasar de 14,101 hogares afectados a 34,237.

El anterior reportaje está muy relacionado con la publicación realizada por el centro de prensa del Programa de las Naciones Unidas para el desarrollo, donde muestra las estadísticas relacionadas con las estafas y lo que han impactado los hogares costarricenses (Programa de Naciones Unidas, 2019).

Por otra parte, una encuesta del INEC (2018) menciona que la estafa por internet es la incidencia que más creció en el país en los últimos años

> Se cita un estudio de la última Encuesta Nacional de Hogares estimó que entre junio del 2017 y julio del 2018 se registraron 55.296 fraudes, esto significa un aumento de un 242,86% con respecto a 2014, es decir pasó de 14.101 hogares afectados a 34,237 hogares afectados por la estafa en internet.

Otro de los pilares de referencia es el incremento de las denuncias por estafas, fraudes o timos según la fuente oficial del OIJ. Grosser (2020) señala en *Delfino Cr* que en la categoría de fraude los mayores incrementos relativos se dieron en timos y estafas informáticas, que aumentaron un 41% y 58% respectivamente, debido a una ingeniería social fuerte en el país.

Por otra parte, la tesis de grado titulada *Fraude bancario en algunos países de Latinoamérica en los últimos tres años, y una guía para el auditor financiero forense* (Rodríguez, 2020) determina la situación del fraude bancario en los últimos tres años en algunos países de Latinoamérica, y confecciona una guía para el auditor financiero forense. A lo largo de la investigación se consultaron estudios globales, artículos periodísticos, blogs, revistas, tesis, que se consideraron fuentes secundarias, y que lograron complementar los resultados que se obtuvieron de las entrevistas a los expertos en el campo.

A continuación, se presentan dos infografías que presentan una radiografía del fraude bancario en algunos países de Latinoamérica y su incremento en la región.

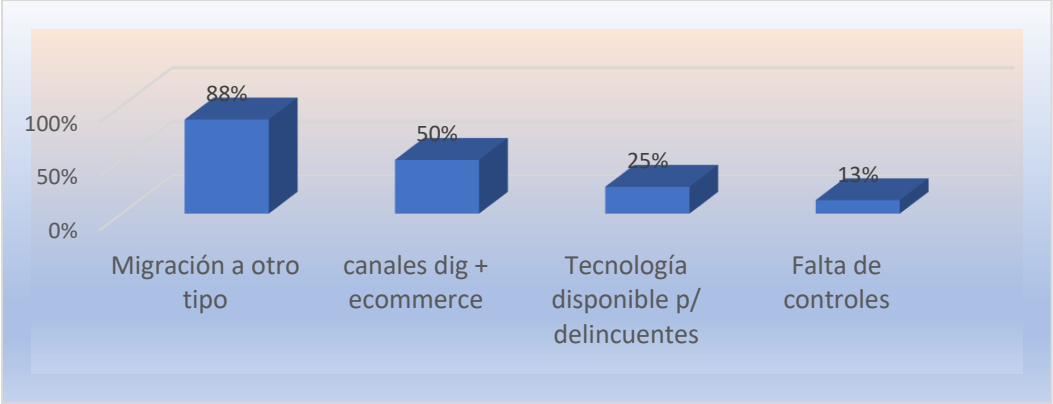
Figura 5. Fraude bancario en AL. Recuperado de: Rodríguez, 2020.

Por otra parte, se presentan los resultados obtenidos a través de la aplicación de la entrevista a las personas especialistas en los temas de la presente investigación.

Sobre el incremento del fraude

El 75 % de los entrevistados indica que el fraude se ha incrementado, y un 25 % señala que más bien el fraude ha migrado.

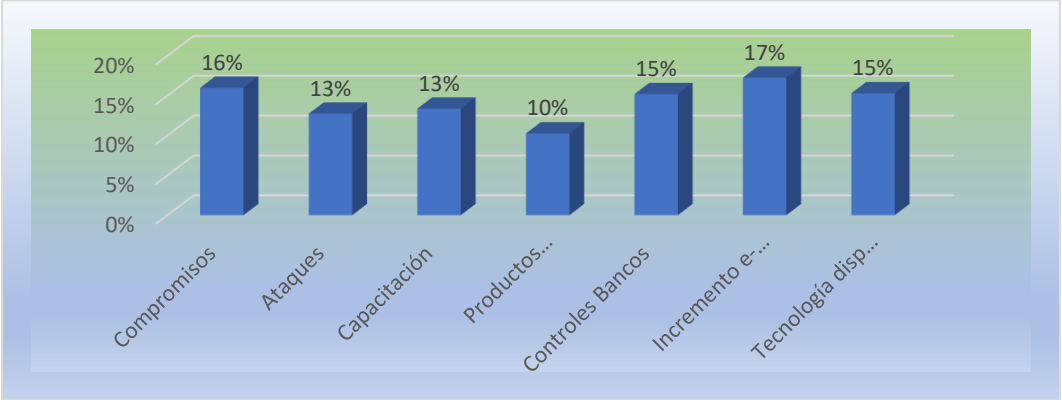
Gráfico 1. Razones del incremento de fraude



Fuente: Elaboración propia, 2021

El gráfico anterior muestra cómo el 88 % de los entrevistados piensa que el fraude migró y, dentro de sus razones se indica que migra de una modalidad menos tecnológica a los fraudes de tarjeta no presente. El 50 % de los entrevistados piensa que el fraude se incrementó por la apertura a más canales digitales y al *e-commerce*, es decir, se diversificó la forma de estafar o de realizar fraude. Esto indica que el fraude migró de una modalidad física a otra virtual. El 25 % expresa que el fraude también ha aprovechado la disponibilidad de nuevas tecnologías a disposición de estafadores. El 13 % señala que el incremento se debe a falta de controles de las instituciones financieras, pues aceptan que los bancos en alguna medida deben mejorar sus controles.

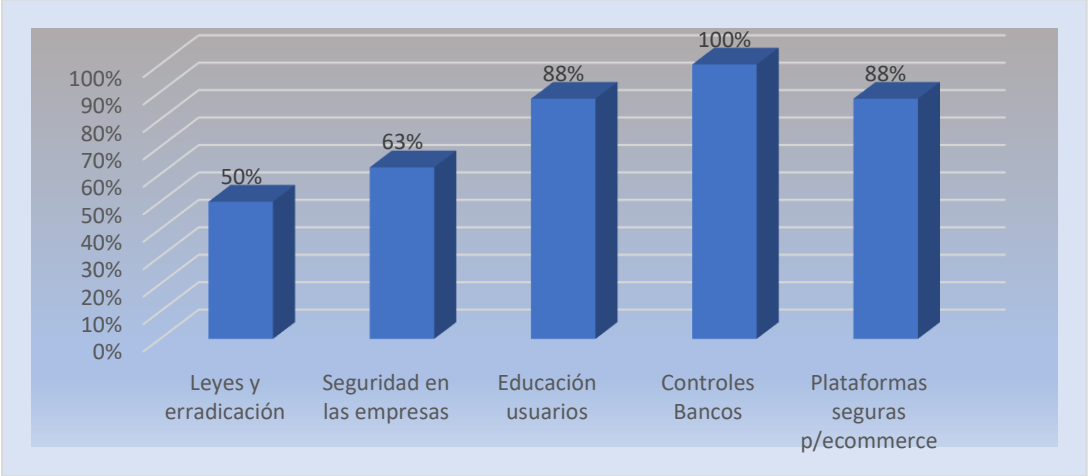
Gráfico 2. Nivel de importancia de las brechas para el incremento del fraude.



Fuente: elaboración propia, 2021.

Este gráfico muestra los tipos de brechas que los expertos consideran tienen una mayor incidencia en el incremento fraude que se cometa. Se observa que una de las causas principales es el aumento en el *e-commerce*, que genera a mayor transaccionalidad, más riesgo de fraude, así como el compromiso de datos, y, por último, la tecnología de punta que favorece a todos los actores, quizá más aprovechada por los estafadores en algunos momentos. En la misma proporción colocan la falta de controles de los bancos y la ausencia de legislación o normativa nacional que respalde al respecto.

Gráfico 3. Importancia de las acciones para mitigar incremento de fraude



Fuente: elaboración propia, 2021

Como se observa, los expertos se inclinan por mayores controles en los bancos (mayor seguridad y sistemas de monitoreo de fraude), mayor educación a los usuarios y mejores plataformas (comercio seguro) para el *e-commerce*. Las plataformas seguras para *e-commerce* tienen que ver con que el cliente tenga que utilizar códigos de seguridad, autenticación, *call back* del banco y otros; sin embargo, tienen un costo para los comercios. Por ello, la mayoría no lo implementa. No se muestra que consideren que otras leyes colaboran en la disminución del fraude, posiblemente, porque los fraudes por Internet son muy difíciles de individualizar.

5. Discusión

La tecnología avanza a un ritmo imparable y es de necios pensar que se puede detener. Como profesionales en derecho, no queda otra opción que seguir especializándose en este terreno, e intentar inculcar este sentido de prevención que debería existir a la hora de creación de cualquier nueva tecnología. Al igual que ocurre en las políticas públicas de seguridad, estas mantienen un

ciclo con diferentes fases (diseño, implementación, entre otras) y por supuesto su evaluación, control y evolución. (Nieto, 2019)

Los fraudes como el *carding* y friendly fraud, además de que son de reciente crecimiento, aprovechan el incremento de las transacciones por Internet y las nuevas tecnologías haciendo uso de datos y valiéndose de que gran parte de los bancos no estaban listos, y no manejan aún sistemas que puedan contrarrestar este tipo de ataques, por lo que urgen los sistemas de perfilamiento de clientes.

Con respecto a la situación del fraude, aun y cuando se entiende que se migró de un mundo físico a uno virtual, el volumen de transacciones por Internet despertó muchas tecnologías, que aparecen día con día, por lo que los actores deben actualizarse en los retos de este nuevo mundo comercial. Muchos clientes, faltos de malicia, requieren la capacitación, sobre todo en banca en línea para tratar de evitar la ingeniería social, aunado a los productos vulnerables de los bancos, como plataformas de banca en línea débiles y falta de sistemas robustos de monitoreo (perfilamiento), lo que abre la posibilidad (brechas) de que estos fraudes, conceptualmente recientes, hayan aumentado.

Existe la necesidad de incrementar mejores y mayores controles, productos, sistemas de monitoreo de fraude y personal para realizarlo. Por esto es importante determinar si una razón del incremento, se debe a que la migración de la modalidad tomó a los bancos con algunos controles obsoletos.

Es probable que la falta de controles tiene que ver con falta de monitoreo transaccional y controles de seguridad en sus plataformas. Por lo tanto, para no sufrir robos de información o exposición de datos, es necesario poseer controles robustos en sus productos, dar capacitación a sus clientes, y otras acciones.

Los ocho entrevistados consideran que para cada canal existen brechas que originan el incremento. Por ejemplo, el cliente tiene un grado de responsabilidad muy alto en los tipos de fraude. Los comercios tienen brechas también y del mismo modo, las transacciones *e-commerce*. En esta pregunta, dejan al banco con un porcentaje menor de brechas. Se podría considerar que según su criterio, la falta de conocimiento del cliente, las debilidades que exponen los mismos comercios *online* y el comercio en general colaboran para que exista más fraude, en comparación con los controles deficientes de los bancos.

La siguiente tabla ayuda a enumerar los conceptos más relevantes en cada una de las fuentes de información y se determinan cuáles se repiten.

Cuadro 1. Comparación de resultados de fuentes de información primaria y secundaria.

Comparación de Resultados de fuentes de información, Razones incremento del fraude.

Coincidencias en Análisis	Conclusiones de las fuentes Primarias	Conclusiones Fuentes Secundarias
Migración e incremento del fraude en algunos países de Latinoamérica	El fraude migró de anteriores tipologías como la Falsificación al mundo del tarjeta no presente (e-commerce) donde se presenta el Account Take Over, Carding, Phishing, quienes aprovechan este canal y las brechas existentes para crecer	Existe un incremento en los fraudes como Carding, Phishing, ATO
Compromiso de datos	El compromiso de datos a Bancos, procesadores, comercios afecta la industria, es uno de los factores que promueve el incremento de fraude	El acceso a sitios no seguros y compromiso de datos se menciona como una de las razcones para el incremento de los fenómenos de fraude.
Falta de capacitación a clientes	Se menciona por parte de los expertos en varias ocasiones, y son concientes que los bancos deben aportar más en este aspecto. También la importancia de que el cliente participe de la capacitación y el enrolamiento a nuevas seguridades.	Se menciona la falta de capacitación como una de las variables que aprovechan los estafadores para el ATO, y el Phishing, la ingeniería social.
Nuevas Teconologías	Los expertos mencionan las nuevas tecnologías disponibles no solo para los bancos, sino para los estafadores, quienes muchas veces llegan primero a utilizarlas para generar fraude.	Las fuentes secundarias mencionan la tecnología de punta como uno de los factores que propician no solo el crecimiento del e-commerce, también el fraude.
Debilidades en los mismos actores (Clientes, Bancos, Comercios)	Se mencionan brechas de capacitación, brechas en los mismos bancos en temas de control, seguridad, sistemas de monitoreo, y en los comercios también.	Se mencionan brechas de capacitación a clientes, debilidades en los sistemas de monitoreo de los bancos (controles), debilidades en plataformas y productos bancarios.
Cyber Crimen especializado	Se menciona que el estafador migró y se expecializó.	Se menciona el compromiso de datos, la ingeniaría social, el phishing, temas en los que el estafador llega primero que el banco o cliente.
Ataques de fuerza bruta	Se menciona como uno de los temas que afectan más al banco, a sus clientes, por medio del fraude carding.	Se menciona la falta de capacitación como una de las variables que aprovechan los estafadores para el ATO, y el Phishing, la ingeniería social.

Fuente: Rodríguez, 2020.

Del cuadro anterior, se logra evidenciar el hecho de que una parte del fraude ha migrado (antiguas tipologías se movieron a tarjeta no presente), y otra parte se ha incrementado por el mismo aumento que ha tenido el comercio por Internet. Por ejemplo, una parte del fraude que se gestionaba como falsificación migró rápidamente, de chip, a fraude de tarjeta no presente. El *carding* y el *account take over*, no solo crecieron por esta migración, sino también por los fenómenos de compromisos de datos, los cuales han sufrido grandes comercios, procesadores y bancos. A raíz de estos diferentes y emergentes tipos de fraude, los bancos reciben ataques de fuerza bruta, que muchas veces, los sorprenden con bajos controles (monitoreo) o con productos débiles.

Por otra parte, la falta de capacitación de los clientes hace que ellos expongan sus datos, ingresen a productos vulnerables o expongan sus datos, y se vuelve al ciclo de los compromisos de datos, donde no solo se presta para los fraudes mencionados en el párrafo anterior, sino también en fraudes como *phishing* y sus derivados, donde el cliente entrega toda su información sensible.

Todo lo anterior se conjuga dentro de un sistema de pagos en donde las transacciones digitales han aumentado muchísimo; sobre todo en épocas de pandemia (COVID-19), y el surgimiento de nuevas tecnologías que favorecen, muchas veces, a los estafadores antes que a los bancos.

En cuanto al monitoreo transaccional, este es necesario para un banco, procesador o adquirente, debido a que, en los últimos tres años, de acuerdo con lo estudiado en este capítulo y, sobre todo para el tipo de fraude de *carding*, *account take over* o banca en línea, los ataques secuenciales son tan fuertes hacia los bancos o procesadores que si no tienen monitoreo transaccional (puede ser subcontratado), los niveles de fraude pueden salir del apetito de fraude definido por las altas gerencias.

Cuando se habla de monitoreo de fraude, se debe implementar para todos los productos del banco, sea cartera de tarjetas de crédito, débito, comercios afiliados, transacciones de banca en línea y todos los productos que generen un riesgo para la institución.

Existen muchos avances en el tema de monitoreo de fraude, los sistemas actuales y, a la luz del dinamismo del fraude, se dirigen especialmente, a actuar con modelos matemáticos que recomienden, con base en las tendencias del fraude, estrategias para defenderse del fenómeno.

Como se mencionó antes, el nivel de monitoreo de transacciones depende del apetito de fraude de la alta gerencia y lo definen de acuerdo con el nivel de fricción que quieren causar al cliente, pues, si tienen un monitoreo más fuerte con estrategias de defensa más robustas y fuertes, deben cuidar la tasa de rechazo de transacciones, que afecta a los clientes y su propio negocio.

6. Conclusiones y Recomendaciones

Al finalizar el presente trabajo de investigación se concluye que el fenómeno del fraude se encuentra asociado al incremento del comercio electrónico y pagos digitales, pues la misma industria al cerrar brechas en el ambiente físico, obliga a los estafadores a migrar a cyber crimen, y a aprovechar nuevas brechas en clientes, bancos, comercios, y procesadores. Estas se presentan por falta de seguridad en algunos de los actores de este ecosistema, propiciando el robo de información y el compromiso de datos, insumos necesarios para los ataques a las instituciones en el ambiente de e-commerce o en el mundo de los pagos digitales.

Una parte del fraude migró hacia otras modalidades cuando se cierra una brecha por parte de la industria de tarjetas, como la colocación de un chip en los plásticos. El fraude migra hacia las transacciones de comercio electrónico, y aparecen tendencias más fuertes. Otra parte importante es que las nuevas tipologías se incrementan apoyándose en la tecnología.

El compromiso de datos es una de las fuentes principales de negocio para los estafadores. Se genera por la baja seguridad en infraestructura y aplicativos de comercios o de bancos; así logran ingresar y obtener datos de los clientes, que después comercializan o utilizan para atacar a los bancos con transacciones fraudulentas, difíciles de identificar. Esto señala que el ciber crimen se ha especializado para realizar fraude bancario y que los ataques de fuerza bruta sorprenden a las instituciones, poco preparadas, para esto.

El crecimiento en las transacciones por Internet genera que el estafador se mueva al manejo de estas tecnologías de una forma veloz, a veces más que los bancos de la región; y descubriera portillos en los productos y plataformas que le permiten atacar y perpetrar fraude, al menos hasta que el cliente, el banco, o el comercio se percaten y mitiguen sus propias brechas.

Este fenómeno exige a los estafadores moverse de región, pues conforme una se vuelve más robusta, se mueven a otra más vulnerable. Por ende, el monitoreo basado en modelos matemáticos y perfilamiento de clientes son un reto para las instituciones, además de acompañarlo con educación y seguros.

Con respecto a las tipologías de fraude bancario con mayor incidencia utilizadas en la región latinoamericana, según su modo de operación y crecimiento en los últimos tres años, se establece que los fraudes que están impactando de forma más fuerte son el *carding*, *account take over* (posicionarse de una cuenta), *phishing* y el *friendly fraud* (fraude amistoso). Para todos estos tipos de fraude, se explicó su operativa, se logró determinar su comportamiento y su impacto, y se confirmó lo mencionado por los expertos entrevistados, por lo que el primer objetivo fue alcanzado satisfactoriamente.

Por otra parte, después de ver los resultados de las preguntas efectuadas a los encuestados, se pueden destacar las conclusiones más importantes:

1. Todos los encuestados coinciden en que existe un incremento en el fraude en América Latina y otras regiones; sin embargo, se menciona que gran parte es el mismo fraude, que migró a otras modalidades como el de con tarjeta no presente.
2. El compromiso de datos tiene una relación muy fuerte con este incremento.
3. El ciber crimen se ha especializado para realizar fraude bancario.
4. Los ataques de fuerza bruta sorprenden a las instituciones, poco preparadas, con productos o sistemas de monitoreo débiles.
5. El crecimiento está ligado con nuevas tecnologías y su uso para generar fraude.
6. Los estafadores se mueven de región, conforme una región se vuelve más robusta, se mueven a una región más vulnerable.
7. Debido a la continua evolución del fraude, las instituciones financieras deben evolucionar igual de rápido en controles para mitigar este riesgo, pues tienden a ser reactivas, hasta que sufren fraude.
8. No existe una política pública en materia de derecho informático que permita sancionar este tipo de conductas ilícitas en forma robusta, inmediata y que sea exigente; lo que hace más que evidente la urgente necesidad de una reforma en la política pública del MICITT ante el incremento de los delitos cibernéticos en Costa Rica, producto de la pandemia del Covid-19.

Lo anterior evidencia, asimismo, el hecho de que el ciber crimen se ha especializado en tratar de atacar con diferentes tipos de fraude, aprovechando las bases de datos que nacen de los compromisos, o de otros métodos como el uso de robots para inferir numeraciones de cuentas, todo esto para tratar de buscar productos en los que puedan monetizar fácilmente, y obtener sus ganancias en servicios o en productos que se comercializan por el Internet.

Referencias

Acevedo, A. (2013). *repositorio.ucsg.edu.ec*. Recuperado de repositorio.ucsg.edu.ec: http://repositorio.ucsg.edu.ec/handle/3317/1000

Aguirre, A. (2017). *Ciberseguridad en Infraestructuras Críticas de la Información*. Maestría en Seguridad Informática. Buenos Aires, Argentina.

Artavia, S. (24 de setiembre de 2020). Pandemia del Covid-19 dispara las Ciberestafas. *La Nación*.

Calderón, M. E. (2018). *Marco Jurìdico de la Profesión Informática en Costa Rica*. Editorial Universidad de Costa Rica.

Esguerra, L. (2020). *Buguroo*. Recuperado de Buguroo: https://www.buguroo.com/es/blog/porque-la-bancarizacion-de-latinoamerica-puede-originar-un-repunte-en-el-fraude-en-la-banca-online

Florentina, M. (2015). *http://repositori.uji.es/*. Recuperado de http://repositori.uji.es/: http://repositori.uji.es/xmlui/bitstream/handle/10234/161252/TFG_2016_DincaClaudia.pdf?sequence=1&isAllowed=y

Grosser, M. (12 de marzo de 2020). *Denuncias por fraude aumentaron 21.8% en 2019*. Recuperado de https://delfino.cr: https://delfino.cr/2020/03/denuncias-por-fraude-aumentaron-21-8-en-2019

KPMG. (2019). *https://home.kpmg/cr/*. Recuperado de https://home.kpmg/cr/: https://home.kpmg/cr/es/home/tendencias/2019/07/fraude_bancario.html

Nieto, J. M. (2019). *Ciberseguridad para un criminólogo*. Cronicaseguridad.com. Recuperado de https://cronicaseguridad.com/2019/08/21/ciberseguridad-para-un-criminologo/

Programa de Naciones Unidas. (19 de mayo de 2019). *https://www.cr.undp.org/*. Obtenido de https://www.cr.undp.org/: https://www.cr.undp.org/

Programa Sociedad de la Información y del Conocimiento de la Universidad de Costa Rica. (PROSIC-UCR). (2010). *Ciberseguridad en Costa Rica*. Universidad de Costa Rica. Recuperado de http://www.prosic.ucr.ac.cr/sites/default/files/documentos/ciberseguridad_2010.pdf

Rodríguez, E. (2020). *Fraude bancario en algunos países de Latinoamérica en los últimos tres años, y una guía para el auditor financiero forense*. Trabajo final de graduación para optar por el posgrado de Maestría profesional en auditoría financiera forense. Maestría profesional en auditoría financiera forense. Universidad Autónoma Monterrey. Costa Rica.

Salas, Y. (19 de setiembre de 2019). Ticos sufrieron 55000 estafas por internet en un año, según INEC. *La Nación*. Recuperado de https://www.nacion.com/sucesos/seguridad/ticos-sufrieron-55000-estafas-por-internet-en-un/7BF2FBPV6VG7HFXZVOJCL4FI2E/story/

Vidal, A. (octubre de 2019). RiskField. Recuperado de: https://www.riskified.com/resources/article/los-fraudes-de-pago-que-estan-de-moda-en-latinoamerica-en-el-2019/

Vukova, C. (19 de mayo de 2020). Ecommerce Fraud Statistics. Recuperado de: Linkedin.com

Anexo 1. Formato de Entrevista

Universidad Latinoamericana de Ciencia y Tecnología (ULACIT)
Licenciatura en Derecho
Entrevista
Tema: ***la necesidad de una reforma en la política pública del MICITT ante el incremento de los delitos cibernéticos en Costa Rica, producto de la pandemia del Covid-19.***

A continuación, encontrará algunas preguntas de desarrollo, y otras de marcar con "X" y completar un porcentaje (%) que se le solicitará de acuerdo con el peso o importancia que usted como especialista considere oportuno indicar.

Se le agradece contestar las preguntas de acuerdo con su experiencia y conocimientos adquiridos en su carrera en prevención de fraudes, y tomando en cuenta las nuevas tendencias de fraude.

1) ¿Considera usted que el estado del fraude bancario en la Región de América Latina y Norteamérica, se ha incrementado en los últimos tres años y por qué? Favor tomar en cuenta o en consideración, las migraciones a chip, nuevas tecnologías, etc.

SÍ	NO	¿POR QUÉ?

2) Si le planteáramos que el universo de actores que intervienen en los servicios bancarios está compuesto por: a) clientes o usuarios de dichos servicios, b) las propias instituciones bancarias, c) los comercios afiliados a los sistemas de pagos bancarios, d) y el mismo mundo de pagos digitales o comercio en internet, e) las políticas públicas en materia de derecho informático; ¿considera usted que en cada uno de ellos existen brechas que colaboran a que el fraude se incremente? ¿Cuáles tipos de brechas hay según su opinión?

Participante en el servicio	SÍ	NO	¿Qué tipo brecha existe y por qué razón? Sea conciso en su respuesta.
Cliente o usuario			
Banco o entidad bancaria			
Comercio			
Ecommerce o pagos digitales			

3) Se le presenta una tabla con diversos tipos de fraude bancario y su grado de afectación a estos actores, favor indique de acuerdo con su experiencia, en cuáles de ellos se tiene o presenta un grado de responsabilidad de que el fraude se cometa.

Participante en el servicio	Carding	Account take over	Ingeniería social/phishing y otros relacionados	Friendly Fraud	Fraude en Comercios	Robo

Cliente o usuario						
Banco o entidad bancaria						
Comercio						
Ecommerce o pagos digitales						

4) De acuerdo con lo anterior, cuáles de estas variables considera usted que colaboran en el incremento del fraude bancario. Marque con una equis (X) y agregue un porcentaje del 1 al 100% (donde 1 es el mínimo y 100 es el máximo), para que lo diferencie de las otras variables y permita generar una categorización o clasificación.

Compromiso de Datos por parte del usuario, cliente o de la entidad bancaria	Ataques secuenciales a grupos de tarjetas, hackeos al azar	Falta de capacitación de los usuarios y clientes	Productos bancarios vulnerables	Falta de controles por parte de los Bancos	Incremento de las transacciones digitales en todos los productos y canales	Tecnología de punta disponible tanto para Bancos como para estafadores

5) Marque con equis “X” las acciones para mitigar el incremento de un fraude bancario se puede realizar por medio de las siguientes acciones. (puede marcar más de una opción o enumerar otra):

Mejor la normativa nacional, construir políticas públicas en materia de derecho informático y tipificar los delitos para su adecuada sanción y/o erradicación	Potenciar y promover una mayor seguridad en la seguridad de las empresas	Promover una mayor educación y sensibilización de los usuarios y clientes bancarios	Implementar mejores controles de las entidades financieras y sus plataformas (monitoreo y productos)	Aplicar e implementar mejoras en la seguridad del acceso y uso de plataformas en los comercios de e-commerce

6) ¿Considera usted que el fenómeno de fraude bancario es común en toda la Región de América Latina, y Norte América, y dónde considera usted que se inicia este crecimiento?

SI	NO	¿POR QUÉ?

Muchas gracias por su colaboración.

Fuente: Rodríguez, 2020; modificada por Zamora, 2021.