Análisis espacial del ciberfraude al comercio electrónico: consideraciones en agenda política Tamaulipeca

Spatial analysis of cybercrime to e-commerce: considerations for political agenda in Tamaulipas

Rosa Amelia Domínguez Arteaga [1], Rodrigo Vera Vázquez [2]

INFORMACIÓN DEL ARTÍCULO

Fecha de recepción: 17 de Diciembre de 2021.
Fecha de aceptación: 7 de Abril de 2022.

[1] Doctora en documentación, Universidad Carlos III de Madrid. Docente-investigador, El Colegio de Tamaulipas-México.
E-mail: rosa.dominguez@tam.gob.mx
Código ORCID:
https://orcid.org/0000-0002-7844-4723

[2] Doctor en Ciencias Sociales, El Colegio de Michoacán. Docente-investigador, El Colegio de Tamaulipas-México.
E-mail: rodrigo.vera@tam.gob.mx
Código ORCID:
https://orcid.org/0000-0001-9200-4428

CITACIÓN: Domínguez Arteaga, R., & Vera Vázquez, R. (2022). Análisis espacial del ciberfraude al comercio electrónico: consideraciones en agenda política Tamaulipeca. Podium, 41, 21–40.
doi:10.31095/podium.2022.41.2

ENLACE DOI:
http://dx.doi.org/10.31095/podium.2022.41.2

Resumen

En un acercamiento hacia la comprensión y atención de la ciberdelincuencia en México, el objetivo es realizar un recuento de las técnicas utilizadas por los ciberdelincuentes, y determinar la distribución espacial del ciberfraude contra el comercio electrónico en Tamaulipas. Metodológicamente se realizó un análisis de las llamadas a la Policía Federal por ciberdelitos de 2018 a 2019 aplicando el coeficiente de localización. Los resultados mostraron que existe concentración de llamadas en Nayarit, Jalisco y Chihuahua. Tamaulipas se colocó como un lugar propenso para este ciberdedelito en el contexto nacional. Las técnicas utilizadas por los ciberdelincuentes fueron principalmente el uso de las redes sociales para robar contraseñas. Se concluye que se requiere de políticas públicas nacionales y locales que atiendan el aumento de los ciberdelitos y la concentración de estos, como fue el caso de Tamaulipas.

Palabras Clave:
Ciberfraude, comercio electrónico, política TIC, ciberseguridad, Tamaulipas, México.

Clasificación JEL: E5, E650, H100.

Abstract

In an approach toward the understanding and attention of cybercrime in Mexico and Tamaulipas, the objective is to make a compilation of techniques used by hackers and to determine the spatial distribution of malpractice against e-commerce in the state. Methodologically, an analysis of the calls to the Federal Police for cybercrimes from 2018 to 2019 was carried out by applying the location quotient. The results showed a centralization of phone calls in Nayarit, Jalisco, and Chihuahua. Tamaulipas was positioned as a prone place for this cybercrime within the national context. The hackers' most used techniques were mainly the theft of passwords by social media. It is concluded that public national and local policies that respond to both the increase and concentration of cybercrimes is required, as in the case of Tamaulipas.

Keywords:
Cybercrime, e-commerce, ICT policy, cybersecurity, Tamaulipas, Mexico.

JEL Classification: E5, E650, H100.

ISSN: 1390-5473 e-ISSN: 2588-0969

Introducción

El delito cibernético ha evolucionado a la par de los adelantos tecnológicos. A pesar de los beneficios que derivan del uso de las Tecnologías de la Información y las Comunicaciones (TIC), su contraparte -una serie de perjuicios materiales e intangibles, ocasionados por los llamados programas maliciosos- pone en alerta a las autoridades, empresas y ciudadanía en general.

Una mirada a la realidad estima que en plataformas digitales como internet, suceden la mitad de los delitos contra la propiedad en el mundo, afectando mayoritariamente al sector de servicios financieros. En consecuencia, los gastos generados por estos ciberdelitos alcanzan grandes cifras para las naciones (Banco Interamericano de Desarrollo y Organización de los Estados Americanos (BID y OEA, 2020), resultando en la implementación de una serie de estrategias que abonen a la atención de dicha problemática.

Asimismo, se ha reconocido que la prevención de la criminalidad es un elemento impostergable para alcanzar el desarrollo sostenible. En ese sentido, las Naciones Unidas (2015) refieren que, en un mundo digital e interconectado, focalizar el carácter transnacional de la delincuencia se convierte en un desafío para los países. Más aún en situaciones como la presente contingencia sanitaria ocasionada por la pandemia SARS-COV2 por la cual ciertas actividades en línea, como el comercio electrónico, han repuntado enormemente (UNCTAD, 2020).

Se afirma que el perfil económico de los compradores cambió bajo este contexto. Ahora, usuarios de hogares con menos recursos monetarios se sumaron a la lista de consumidores de productos y servicios en línea (UNCTAD, 2020). Ampliándose así el público vulnerable a la ciberdelincuencia.

En 2019 en México, ocho de cada diez usuarios de internet mayores de edad habían realizado una compra en línea (Asociación de Internet MX, 2019b). Esto fue equivalente a 46 % de los usuarios -mismos que están en riesgo de sufrir un ataque cibernético. Donde, una de cada cuatro personas ha sido víctima de cibercrimen (McKinsey & Company-Comexi, 2018).

En el tercer trimestre de 2019 los reportes por fraude cibernético aumentaron casi 40 % (el doble que los delitos tradicionales) (Notimex, 26 enero de 2020), siendo en su mayoría aquellos relacionados con el comercio electrónico (96 % del total). De hecho, se ha identificado que este es el ciberdelito con mayor presencia en el país (Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros - Condusef, 2018).

En relación con el tratamiento de estos actos delictivos, aún persisten varios aspectos por considerar. Uno de ellos es ahondar en los tipos de ciberdelitos y su repercusión en la sociedad, incluso en su incorporación dentro de la agenda gubernamental. En la indagación resulta

PODIUM No. 41, Junio 2022, pp. 21-40

ISSN: 1390-5473 e-ISSN: 2588-0969

de interés identificar regiones de concentración de dichos actos específicamente el fraude al comercio electrónico. La falta de atención a este nicho podría suponer una serie de implicaciones negativas como una mayor dificultad al tratamiento legal de dichas acciones, haciendo que la sanción adquiera complejidad y obstaculice la lucha contra la expansión del fraude al comercio electrónico, por mencionar solo algunas (Acosta et al., 2020).

En Tamaulipas el comercio electrónico va en aumento; el ciberfraude se sitúa como uno de los delitos de mayor crecimiento. Debido a la evidencia de actividad ilícita en el país, la Policía Cibernética de la Policía Federal, inició sus funciones en la entidad en el año 2018. El objetivo fue atender los ciberdelitos toda vez que se recibía un número significativo de denuncias por esos hechos (Hernández, 13 de julio de 2018) y en la actualidad, no es la excepción (Hernández, 31 de marzo de 2021).

Por lo anterior, el objetivo de la presente investigación es determinar la distribución espacial del fraude cibernético contra el comercio electrónico por entidad federativa a través de un coeficiente de localización. Con ello, demostrar que Tamaulipas se ubica en el comparado nacional como un territorio con alta concentración de denuncias relacionadas con este fraude. Con la aproximación se busca generar evidencia para contribuir en la conformación paulatina de estrategias vinculantes de atención y prevención de la problemática.

El estudio es descriptivo con alcance exploratorio, pues no se cuenta con suficientes antecedentes de investigaciones similares enfocadas en las entidades del país. Con lo anterior, se cuestiona: ¿qué entidades federativas muestran la mayor concentración de fraude cibernético al comercio electrónico?, ¿cuáles son las técnicas mayormente utilizadas por los ciberdelincuentes para tal fin?, ¿cuál es la magnitud del fraude al comercio electrónico en Tamaulipas? En la entidad, ¿dicho ciberdelito muestra altos niveles de concentración?, es decir, ¿Tamaulipas adquiere relevancia como territorio propenso al fraude al comercio electrónico en el contexto nacional?

Una de las afirmaciones de la que se parte es que las entidades con mayor actividad en el comercio electrónico serán propensas a registrar ciberfraude a través de diversas técnicas. Para el caso de Tamaulipas, se afirma que la categoría de ciberdelitos relacionada con las afectaciones cibernéticas a los bienes patrimoniales coincide con las tendencias que se muestran en otras latitudes, constituyendo así el principal problema en la materia, siendo considerado como lugar propenso a este ciberdelito, ameritando implementar medidas al respecto.

La metodología utilizada se basa en la sistematización documental de fuentes primarias y secundarias. En un primer momento se revisaron los aportes conceptuales y referenciales del tema elegido. Enseguida se estructuró el estado de la cuestión para México y Tamaulipas,

PODIUM No. 41, Junio 2022, pp. 21-40

ISSN: 1390-5473 e-ISSN: 2588-0969

haciendo uso de la información nacional proveniente de fuentes oficiales como la Condusef, y el Instituto Nacional de Estadística y Geografía (Inegi), y de asociaciones de internet en el país. Después, se realizó una base de datos con los registros proporcionados por la Policía Federal a través del Centro de Atención Ciudadana, a los que se aplicó un modelo de análisis geoespacial (el coeficiente de localización) para determinar el nivel de concentración de eventos a escala nacional y para el estado de Tamaulipas. Se exponen los resultados y la interpretación de estos, finalizando con un apartado de conclusiones.

El ciberfraude y el relacionado con el comercio electrónico

El ciberfraude

El ciberfraude, fraude cibernético, fraude informático o estafa cibernética se refiere a "aquellas estafas que utilizan la red, para realizar transacciones ilícitas" (Condusef, 2019, s.p). Según Pecoy Taque (2011) el fraude cibernético es una conducta de delito al comercio electrónico que, junto con la falsificación de documentos electrónicos, la publicidad engañosa y la sustracción de datos personales, ameritan ser castigadas. Así los Estados buscan punirlos desde el derecho penal y comparado.

En los últimos años han resaltado este y otros ciberdelitos con mayor frecuencia en las empresas y organizaciones, lo que supone grandes pérdidas económicas (Peñaloza y Morillo, 2010). Pues generalmente son instituciones financieras o comerciales, y en menores casos el sector público o gubernamental, los más dañados. De forma global, es el resultado del mal uso de equipos y programas (como la destrucción y robo de datos o archivos).

A tenor, desde hace algún tiempo se señalaba que los eventos mayormente presentes en relación a los ciberdelitos eran los fraudes por computadoras o electrónicos (Álvarez, 2020), incluso lavado de dólares con dichas prácticas, la divulgación de claves de acceso o la conexión de equipos no autorizados; acciones que, como opina Téllez "al no estar debidamente recogidas en la legislación penal, propician un incremento en cuanto a su tentativa o consecución" (1996, p. 462). Para este autor, las causas principales de estos delitos son fallas o inexistencia de elementos de control en las empresas, lo mismo que las características propias del personal que opera las computadoras.

Según Estupiñán Gaitán (2002), existen diferentes tipos de ciberfraudes: los que se realizan a las tarjetas bancarias (uso indebido, clonación, exceso de cupo y tarjeta gemela); la suplantación de la razón social y; el *electrónico*. Este último tiene que ver con el "manejo o alteración que pueden realizar una o varias personas al *software* o sistema informático de una entidad con el fin de copiar, cambiar, activar, cancelar, eliminar, aumentar, entre otras, la información relacionada con tarjetas de crédito" (Lara Guijarro y Albán Silva, 2017, p. 67).

Por su parte, Álvarez (2020) establece cinco tipos: *malware* (programa para

PODIUM No. 41, Junio 2022, pp. 21-40

ISSN: 1390-5473 e-ISSN: 2588-0969

dañar el sistema operativo o causar un mal funcionamiento), *keyloggers* (programas maliciosos para capturar la actividad realizada en la computadora), *spyware* (software para monitorear actividades de la víctima desde un acceso remoto), *spam* (envío de correo no deseado para solicitar información) y *hacking* (acceso ilegal a un sistema informático). Estos se señalan en otros trabajos (Quevedo González, 2017) como técnicas para realizar no solamente fraude, sino variados ciberdelitos.

Lara Guijarro y Albán Silva (2017) documentaron aquellos más habituales en otras latitudes. Por ejemplo, en Ecuador se han presentado los relacionados con las claves de banca electrónica de los usuarios, páginas web con ofertas de productos o servicios falsos y la suplantación de identidad. Así mismo, los ciberfraudes en transacciones *online* de compra-venta o alquiler de vivienda, en compra-venta al comprador y al vendedor (EBay), ofertas de trabajo y oportunidades de negocio falsas, redes piramidales, estafa nigeriana, *ransomware* (infección de sistemas informáticos mediante virus que bloquean la computadora) y *phishing* (envío masivo de correos electrónicos mediante spam), fueron documentados en España (Sanz Párraga, 2016).

Así, diversas consultoras y organizaciones señalan que la tendencia de estos actos ha ido en aumento, sobretodo en situaciones como la presente contingencia sanitaria ocasionada por la pandemia SARS-COV2. Dicho momento es aprovechado por los ciberdelincuentes para acceder más fácilmente a datos privados personales y financieros mientras los usuarios se encuentran en busca de alternativas en línea para satisfacer sus necesidades (Arsene, 2020).

Al respecto, según el Informe Anual sobre amenazas para la seguridad en internet realizado por Symantec (2019), el *formjacking* (infectar servidores web para remover información financiera de consumidores) es actualmente el más frecuente entre empresas y organizaciones que se protegen con Symantec. El documento muestra que 4818 sitios *web* únicos se vieron comprometidos con este código cada mes en 2018, para robar datos de tarjetas de crédito. Señalan que, con los datos de tan solo 10 de estas tarjetas robadas, se podría generar un rendimiento de hasta 2.2 millones de dólares mensuales para los ciberdelincuentes.

Otros riesgos presentes en el mismo periodo fueron el *cryptojacking* (amenaza que se oculta en la computadora para extraer monedas digitales) y el *ransomware*. Con lo anterior, la empresa Symantec señaló que la minería, finanzas, seguros y bienes raíces son los sectores de la industria más afectados por estas amenazas.

Las formas más innovadoras utilizan el correo electrónico, redes sociales, páginas web y el sinnúmero de aplicaciones disponibles en internet, y servicios a través de telefonía inteligente y plataformas móviles para engañar, persuadir o motivar errores en las

PODIUM No. 41, Junio 2022, pp. 21-40

ISSN: 1390-5473 e-ISSN: 2588-0969

personas o grupos que hacen uso de dichas herramientas (Avendaño, 2018). Por su parte, Oxman (2013) afirma que el *phishing pharming* (programa que desvía a un consumidor hacia una página electrónica apócrifa) y el *money mules* (mula o mulero que pone a disposición de los estafadores las ganancias obtenidas prestando sus cuentas bancarias y blanqueando el dinero defraudado), son actividades que participan en la estafa informática.

Las vulneraciones se reflejan en grandes pérdidas económicas en las naciones. Como resultado, los daños ocasionados podrían superar el 1% del Producto Interno Bruto (PIB) en algunas naciones (BID y OEA, 2020) como Estados Unidos, Italia y Reino Unido (Arsene, 2020). En adición, puede reconocerse a México entre los más afectados, pues incluso al interior de este, las transacciones ilícitas representan una gran carga onerosa al Estado (Condusef, 2018).

Un estudio de la OEA (2019) señala que 100 % de las entidades financieras en México manifestaron haber experimentado algún evento de seguridad digital en su contra, durante 2018. Los tres hechos más comunes fueron: el *malware* en primer lugar (56%), seguido del *phishing* (47%) y el *clear desk* (violación de políticas de escritorio) (31%). Los dos primeros también se manifestaron en contra de los clientes además de los relacionados con la ingeniería social (obtener información privada de empresas, directivos y empleados, para desviar dinero). El motivo de tales ataques fue mayormente económico, en lugar de las cuestiones políticas, reputación y robo de información personal.

Además, se menciona que México obtiene muy mala calificación en lo que a ciberseguridad se refiere. De acuerdo con la Condusef (s.f.), en 2017 la Unión Internacional de Telecomunicaciones (UIT) colocó a México en el lugar 28 de 193 países miembros en materia de ciberseguridad, por debajo de EU, Francia, Canadá, Rusia, Japón, Israel e India. Aunque, en América Latina, es el país mejor posicionado. Así, en el Estado mexicano una de cada cuatro personas ha sido víctima del cibercrimen (McKinsey & Company - Comexi, 2018).

Para mostrar lo que se vive en México con relación a los ciberdelitos y en especial atención a la estafa cibernética, Avendaño (2018) utilizó el Reporte de Desempeño de las Entidades Financieras de 2018 para destacar que, en el país, de 2011 a 2016, los bancos concentraron 99% de las reclamaciones por parte de los usuarios. En el reporte se hizo notable el incremento en las quejas por fraudes cibernéticos, que aumentaron casi un 800% en dicho periodo en comparación con el fraude tradicional (relacionados con operaciones de banca digital o por internet). Lo que invita a las autoridades a implementar y mantener una estricta vigilancia para evitar estos incrementos, coordinando el trabajo con los prestadores de servicios.

El ciberfraude al comercio electrónico

Si el fraude cibernético está vinculado mayoritariamente con el delito al

PODIUM No. 41, Junio 2022, pp. 21-40

ISSN: 1390-5473 e-ISSN: 2588-0969

comercio electrónico, sería preciso hacerle mención para un mejor entendimiento. De acuerdo con la Organización Mundial del Comercio, la actividad del comercio electrónico es referirse a la "producción, publicidad, venta y distribución de productos a través de redes de telecomunicaciones" (OMC, 2021, s.p.). Debido a la extensión en el acceso y uso de las TIC, el sector económico se ha visto beneficiado con las múltiples transacciones que pueden realizarse con tecnologías como internet.

En ese sentido, el comercio electrónico es una modalidad con innumerables posibilidades de compra y venta de bienes tangibles e intangibles; de cómoda entrega y recepción de productos, cuya transacción monetaria puede ser totalmente digital. En esta pronta consolidación ha crecido de manera sorprendente. Por ejemplo, en 2017 las ventas se elevaron 13 %, con una ganancia de 29 billones de dólares en Europa, Asia y Norteamérica (González García, 2020).

Esta actividad es el resultado de la evolución del comercio tradicional pero además una innovación en la forma de contratar. Las implicaciones son una serie de transformaciones en

> […] los sujetos intervinientes en las transacciones, en el ámbito en que éstas se realizan, en los medios de comunicaciones utilizados por las partes y en los métodos utilizados para asegurar las transacciones. En este sentido uno de los elementos que transformó la actividad comercial de manera sensible fue la incorporación de medios electrónicos. (Ríos Ruíz, 2014, p. 69).

Para algunos, el comercio electrónico es una herramienta innovadora que existe para incrementar la venta de los productos o servicios gracias a que las diversas modalidades de pago pueden usarse durante todo el año, permitiendo a los clientes realizar alguna compra en el momento que lo deseen. A raíz de estos cambios, esta modalidad ayuda a las empresas a crecer más, y posibilitar su competencia ante las grandes y actuales industrias (Hernández Mendoza et al., 2018)[3].

Cabe señalar que el progreso del comercio electrónico se ha desplegado más rápido en países desarrollados, pero está presente aún en los menos avanzados. Para algunos es una actividad que está surgiendo recientemente en dichos contextos, pero que progresa a una velocidad enorme. Por ejemplo, para González García (2020) ha sido la necesidad de importar bienes y servicios tecnológicos; baja productividad; mano de obra poco calificada y escasa tecnología. Por lo tanto, para mejorar su situación deben "contar con una mayor disponibilidad de infraestructura digital, acceso a Internet, alfabetización digital, reforzar las políticas digitales, fomentar la inclusión financiera y contar con acceso a métodos de pago, educación, habilidades, seguridad en línea, logística

[3] En el comercio electrónico intervienen el gobierno, el empresario y el consumidor, clasificándose en comercio electrónico entre empresas (B2B), comercio electrónico entre empresas y la administración (B2A), comercio electrónico entre consumidores (C2C) y comercio electrónico entre gobierno y consumidores (A2C).

PODIUM No. 41, Junio 2022, pp. 21-40

ISSN: 1390-5473 e-ISSN: 2588-0969

y facilitación del comercio" (p. 61).

Tomando en cuenta estas limitaciones, México ha experimentado un crecimiento en el comercio electrónico. En 2009 este representó una suma de 24.5 miles de millones de pesos, mientras que en 2018 sumaron 491.25 miles de millones de pesos, impactando en 5% en el PIB nacional para el mismo año (González García, 2020). Pero aún a pesar de este repunte, fue ubicado en el lugar 93 de 152 países en el Índice de Comercio Electrónico 2020 de la Conferencia de las Naciones Unidas Sobre Comercio y Desarrollo (UNCTAD, 2020), que mide las facilidades de cada país para que sus consumidores puedan realizar compras en línea. Sus debilidades fueron una mala inclusión financiera (falta de acceso a una cuenta bancaria) y la falta de confiabilidad en la capacidad logística (medios de entrega).

Hay investigaciones que reportan las principales limitantes de México en cuestión, como las formas de pago (muy poca población con tarjeta de crédito o débito); pocos usuarios que usan las plataformas de comercio electrónico; desconfianza en los sistemas de información; baja penetración de banda ancha en el país, y los temas de oferta. Además, en relación con las pequeñas y medianas empresas (PYMES) mexicanas, se reporta que 73 % utiliza Internet, pero solo 10 % vende en línea (Hernández Mendoza et al., 2018).

No está por demás mencionar que, de acuerdo con *eComerce Institute* (2012), el fraude en el comercio electrónico cuesta alrededor de 280 millones de dólares en Latinoamérica. Actualmente para cualquier organización que realiza ventas en línea, prevenir el fraude representa un costo adicional, por lo que las compañías de *software* especializadas en diseño de programas de antivirus y anti-espías (*antispyware*) avanzan aceleradamente en el mercado de la ciberseguridad.

En el informe del UNCTAD (2020) se logra visualizar el futuro de la situación al mencionar que casi cuatro de cada diez mexicanos realizaron por primera vez alguna compra en internet en 2019, y que 90 % de ellos continuarán haciéndolo. Dichas propuestas parecen alentadoras, sin embargo, últimamente el principal fraude cibernético que se presenta en México es por medio de esta actividad. En ese sentido, la Condusef (s.f.) indica que, en 2017, 92 % del fraude cibernético fue por comercio electrónico, destacando el aumento de personas físicas como víctimas y de la banca móvil (123 % y 78 % en ese orden) respecto al año 2016. En este último, la instancia registró una cifra de 5 588 casos que calificó de histórica.

Dado lo anterior, la Condusef (2018) apunta que, en el tema, los datos ofrecidos "sugieren una urgente necesidad de que las plataformas de e-commerce cuenten con mecanismos adicionales de autenticación de sus usuarios" (s.p.). Y es que para el tercer trimestre de 2019 los registros en torno al fraude cibernético y al comercio electrónico en México, aumentaron casi 40 % (el doble que los delitos tradicionales) (Notimex, 26 de enero de 2020).

PODIUM No. 41, Junio 2022, pp. 21-40

ISSN: 1390-5473 e-ISSN: 2588-0969

Cabe señalar que esta instancia cuenta con un portal de fraudes cibernéticos en el que brinda información sobre los tipos y cómo prevenirlos. En específico se puede encontrar un monitor de reporte con información de una variedad de actos a través de llamadas (el *vishing*), mensajes de texto SMS, Whatsapp (*smishing*) y suplantación de instituciones financieras (Condusef, 2021b).

Un dato importante que resaltar es que este mercado no solo está abierto para empresas como oferentes, sino que se ha convertido en una opción para las personas físicas que mantienen un negocio.

Se estima que la situación de contingencia actual ha originado que actividades como estas vayan en aumento. De hecho, la tasa de personas que trabajan por cuenta propia en México mostró un incremento en el año 2020 (Inegi, 2021). Así, un nuevo grupo de pudiera estarse perfilando como blanco de ciberataques que quedaban fuera como parte de las desigualdades de la sociedad de la información.

Con relación al contexto del delito al comercio electrónico en Tamaulipas, durante el primer semestre de 2021, la Condusef registró 1 672 controversias en la entidad, donde la transferencia electrónica no reconocida figuró entre las tres principales causas de estas. Estas quejas, y la negativa a cumplir con la conclusión anticipada establecida en el contrato y los consumos no reconocidos representaron 40 % del total. Los municipios de Tampico y Ciudad Madero concentraron 35 % del total de éstas (Condusef, 2021a). Se infiere, que estas transacciones pudieron haber terminado en fraude por compras en Internet.

De acuerdo con esto, algunos estudios indican que los principales asuntos pendientes (problemas) en torno a la estafa electrónica son: una problemática teórica general conceptual que está relacionada con el comercio electrónico; aristas legales que hay que pulir en muchos países y, por último, está atado evidentemente al problema de la educación financiera (Lara Guijarro y Albán Silva, 2017, p. 66).

Por su parte, también se señala la responsabilidad de las entidades financieras que se han visto más afectadas. Al respecto, Rufín Moreno (2002) encontró que no cumplen cabalmente con su función de garante monetario. Para él, las instituciones bancarias solo ofrecen soluciones parciales ante los fraudes cibernéticos, pues a pesar de realizar algunas acciones para reducirlo, falta una estrategia general del sistema monetario ante las fallas de su garantía. En su estudio, Paz Sefair (2018) concluye que las entidades financieras deben hacer todo lo posible para establecer medidas de seguridad y evitar responsabilizar al consumidor. De hacerlo así, el banco se hallaría en un comportamiento culposo.

Una de las recomendaciones es que las instituciones financieras automaticen su proceso de detección de fraudes, esto impide procesar demasiadas transacciones legítimas o bloquear incorrectamente

PODIUM No. 41, Junio 2022, pp. 21-40

ISSN: 1390-5473 e-ISSN: 2588-0969

tarjetas o cuentas genuinas, pues sólo pueden ser revisados un número limitado de transacciones (Álvarez, 2020). Sin embargo, para algunos autores el esfuerzo en la materia va más allá de indemnizar a los clientes o titulares de cuentas bancarias; exigir seguros ante estos atentados; o invertir en campañas de educación. De lo que se trata, en todo caso es

> […] por una parte, reconocer y ponderar las indudables ventajas que tiene para las personas el uso masivo de la tecnología, en una sociedad que ya no concibe su existencia sin ella y, por otra parte, evaluar la necesidad de establecer unos límites precisos, a fin de que ese intercambio de información no amenace con socavar el mantenimiento de las condiciones mínimas que posibilitan la autorrealización individual (Oxman, 2013, p. 214).

A pesar de lo sugerido, se carece de investigaciones académicas que analicen la situación en México y sus implicaciones, y de estudios que realicen una comparativa y posterior discusión de los resultados de una investigación actual, a la luz de lo encontrado por otros autores. Esto se adjudica indudablemente, a que los estudios de internet se consideran emergentes, a escala local e internacional (Inegi, 2015).

Tal vez lo anterior se debe a una falta de claridad teórica con relación al concepto de ciberdelito y las formas de perpetrarlo según la literatura abordada, que pudiera limitar su tratamiento. Un primer intento sería conocer la situación; abordar cómo actúan los ciberdelincuentes y cuáles son las tácticas utilizadas (Cámara Colombiana de Informática y Telecomunicaciones - CCIT, 2019, s.p.). Intención principal del presente texto, cuyos resultados están orientados a coadyuvar también en la atención de la ciberdelincuencia con un enfoque en la entidad de Tamaulipas.

Metodología

Lo información aportada por la Condusef y el Inegi permitió explorar el contexto de los ciberdelitos en el país, específicamente el ciberfraude al comercio electrónico. Así mismo, se usaron datos generados por la Secretaría de Seguridad y Protección Ciudadana de la Policía Federal, a través del Centro Nacional de Atención Ciudadana del 16 de agosto de 2018 al 16 de agosto de 2019. Se tomaron en cuenta 3 506 llamadas en relación con delitos cibernéticos (17 sin especificar estado) y 6 733 reportes, datos que se recibieron como "denuncia ciudadana". Las cifras se solicitaron al Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, utilizando los mecanismos establecidos mediante petición pública.

Para medir la distribución espacial se aplicó a los 6 733 reportes, desglosados por entidad, una técnica de análisis regional: el coeficiente de localización simple que representa la relación entre la participación de una determinada variable "i" en la región "e" y la participación de la misma variable en el total nacional "E" (Isard, 1962).

La aplicación del coeficiente de

PODIUM No. 41, Junio 2022, pp. 21-40

ISSN: 1390-5473 e-ISSN: 2588-0969

localización simple (LQ por sus siglas en inglés) busca determinar la magnitud de una actividad en el territorio objeto de estudio. De esta manera se podría conocer si Tamaulipas adquiere relevancia como territorio propenso al fraude en el contexto nacional.

La fórmula para estimar el coeficiente de localización se expresa de la siguiente manera:

$$LQi = ((e_i / e_t) / (E_i / E_t))$$

Donde:

"ei" es un tipo determinado de denuncia de ciberdelito registrado en una entidad federativa.

"et" se refiere al total de denuncias de ciberdelitos registradas en una entidad federativa.

"Ei" es un tipo determinado de denuncia de ciberdelito registrada a escala nacional.

"Et" se refiere al total de denuncias de ciberdelitos registradas a escala nacional.

Teniendo en cuenta el conjunto de datos registrados a escala nacional, se interpretó lo siguiente: si LQi ≥ 1 entonces existe concentración de denuncias de ciberfraude al comercio electrónico en la entidad federativa. Si LQi < 1 entonces no existe concentración de denuncias de ciberfraude al comercio electrónico en la entidad federativa. Es importante señalar que esta técnica es la que mayormente se ha utilizado en investigaciones para el análisis de la criminalidad (Sánchez Salinas, 2014).

Resultados

En la Figura 1 se observa que de las

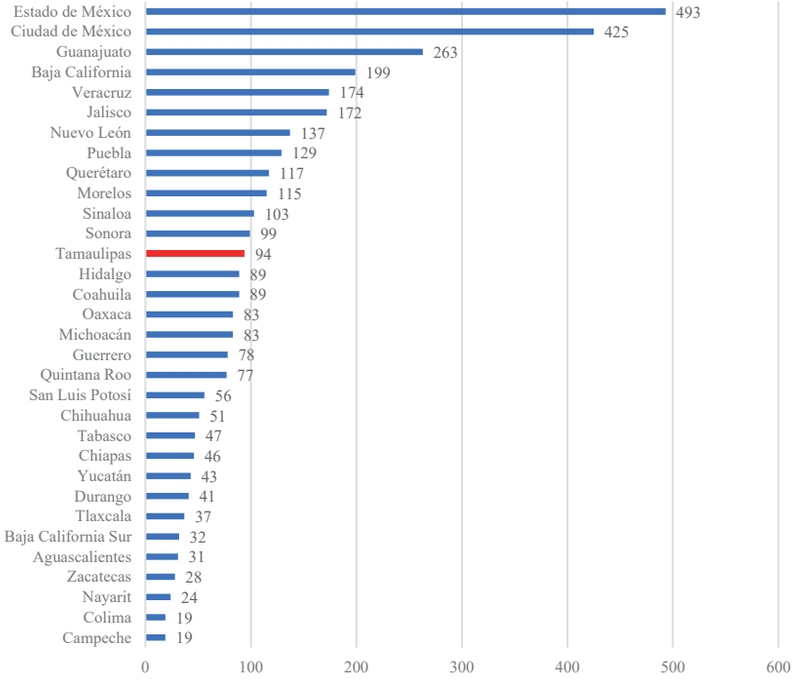

Figura 1. Llamadas por ciberdelitos a escala nacional de agosto de 2018 a agosto de 2019.
Fuente: Elaboración propia con información de la Policía Federal mediante solicitud pública.

PODIUM No. 41, Junio 2022, pp. 21-40

ISSN: 1390-5473 e-ISSN: 2588-0969

llamadas recibidas en relación con ciberdelitos provenían mayormente del Estado de México, Ciudad de México y Guanajuato. Al respecto, Tamaulipas ocupó el lugar número 13 de la lista de llamadas a escala nacional. En comparativa regional, la entidad se posicionó por debajo de Nuevo León, pero por encima de Coahuila.

Las principales técnicas para delinquir en el país (Ver Figura 2) fueron el robo de

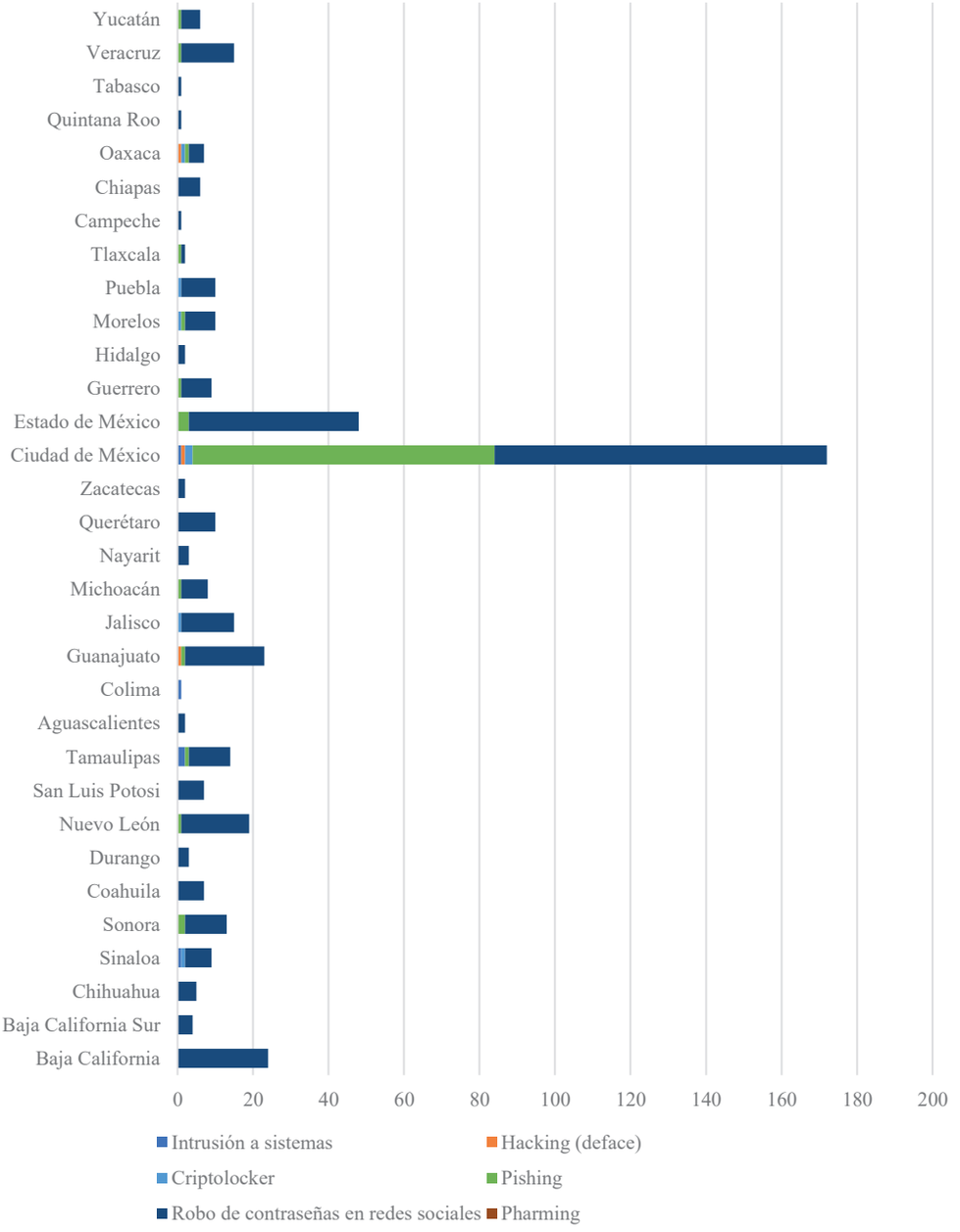

Figura 2. Técnicas utilizadas para cometer ciberdelito en México de agosto de 2018 a agosto de 2019 (según reportes realizados).
Fuente: Elaboración propia con información de la Policía Federal mediante solicitud pública.

PODIUM No. 41, Junio 2022, pp. 21-40

ISSN: 1390-5473 e-ISSN: 2588-0969

contraseña en redes sociales, *phishing* y *criptolocker*. Siendo en Ciudad de México, Estado de México y Baja California donde se presentaron más. En Tamaulipas se siguió la misma tendencia, aunque no hubo registro de llamadas por *criptoloker*, pero se presentó el *phishing*, y se destaca que el delito de intrusión a sistemas se presentó lo doble que el *phishing*.

Del total de reportes registrados en el país, la Policía Cibernética ubicó 32 ilícitos[4] y los distribuyó en cinco categorías: agravio contra personas, fraude y extorsión, eventos de seguridad informática, denuncias de ilícitos varios a través de la *web* y delitos contra menores.

Los resultados demuestran que existe discordancia entre las dependencias oficiales mexicanas y las consultoras internacionales con relación a los tipos de ciberdelitos y las tácticas de ataque. Por ejemplo, la Condusef (2018) considera el *smishing* (Mensajes de texto; SMS, whatsapp) como uno de los principales ciberdelitos; sin embargo, en la lista de la Policía Federal Cibernética se encuentra ausente. Por su parte, Symantec (2019) informó que el *formjacking* ocupa el primer lugar en el mundo, aunque aún no se registra por las instancias mexicanas. Esto sugiere una actualización de registros en conjunto a los avances tecnológicos utilizados por los ciberdelincuentes.

Para el caso de las denuncias registradas como fraude al comercio electrónico -variable que constituye uno de los actos de mayor continuidad y/o presencia en el mundo- es necesario reinterpretar su distribución espacial mediante un patrón de comparación en un periodo determinado. Con ello, estimar el nivel de concentración de afectaciones a las finanzas de las personas físicas y morales que registra Tamaulipas.

En efecto, el acceso a servicios que requieren de operación a través de internet, como la banca *on-line* y/o el comercio electrónico, aumentan cada día permitiendo realizar transacciones de cualquier tipo. Ante ello, la utilización maliciosa de *software* para delinquir se concentra particularmente en entidades como Nayarit, Jalisco y Chihuahua. Si bien, Tamaulipas no figura entre los 10 primeros estados con registro de denuncias (ver Figura 3), sí arroja resultados por arriba de la media nacional y según la puntuación obtenida (Si LQi $\geq$ 1), existe concentración de denuncias de este tipo de ciberdelito.

Es de llamar la atención que Tamaulipas se ubicó en dicho coeficiente por encima de entidades como el Estado de México y Ciudad de México, que fueron blanco de mayor ataque, sin decir que poseen altos niveles de concentración de llamadas o que sean más propensos a este delito. Es importante señalar que

[4] Acoso, Amenazas, Difamación, Suplantación de identidad, Extorsión, Fraude al comercio electrónico, Fraude al usuario de la banca electrónica, Fraudes diversos, Fraude nigeriano, Intrusión a sistemas, *Hacking (deface), Malware, Anti/shildporn spam protection 2.0, Criptolocker, Pishing*, Robo de contraseñas en redes sociales, *Pharming* , Reporte ciudadano de páginas *web*, Acoso contra menor de edad, Amenazas contra menor de edad, *Ciberbullying*, Corrupción contra menor de edad, Desaparición de menor de edad, Difamación contra menor de edad, *Grooming, Sexting*. Otros informativos preventivos, Pedofilia. Pornografía Infantil, Robo de contraseñas en redes sociales, Suplantación de identidad y Trata, los últimos contra menores de edad.

PODIUM No. 41, Junio 2022, pp. 21-40

ISSN: 1390-5473 e-ISSN: 2588-0969

estas entidades son parte de la zona centro del país, donde se ubica el mayor número de cibernautas y compradores en línea del país (25 %), de acuerdo con la Asociación de Internet MX (2019b).

Con el coeficiente de localización se logra observar la vulnerabilidad de ciertos territorios en términos de ciberfraude, toda vez que la ponderación de datos enseña concentraciones (registros) que rebasan al componente relativo nacional. Al respecto, Sánchez Salinas (2014) utilizó esta herramienta para estudiar el delito en tres

Este autor encontró en su revisión bibliográfica que "el crimen no está distribuido aleatoriamente en el espacio si no que está íntimamente asociado con el entorno físico en el que se produce, por lo que los patrones geográficos del delito se pueden asociar estadísticamente a las condiciones estructurales y la composición social de las diferentes áreas que conforman a las ciudades" (Sánchez Salinas, 2014, p. 3).

Por lo tanto, se puede establecer que dicha concentración del ciberdelito dependerá de múltiples factores. Una

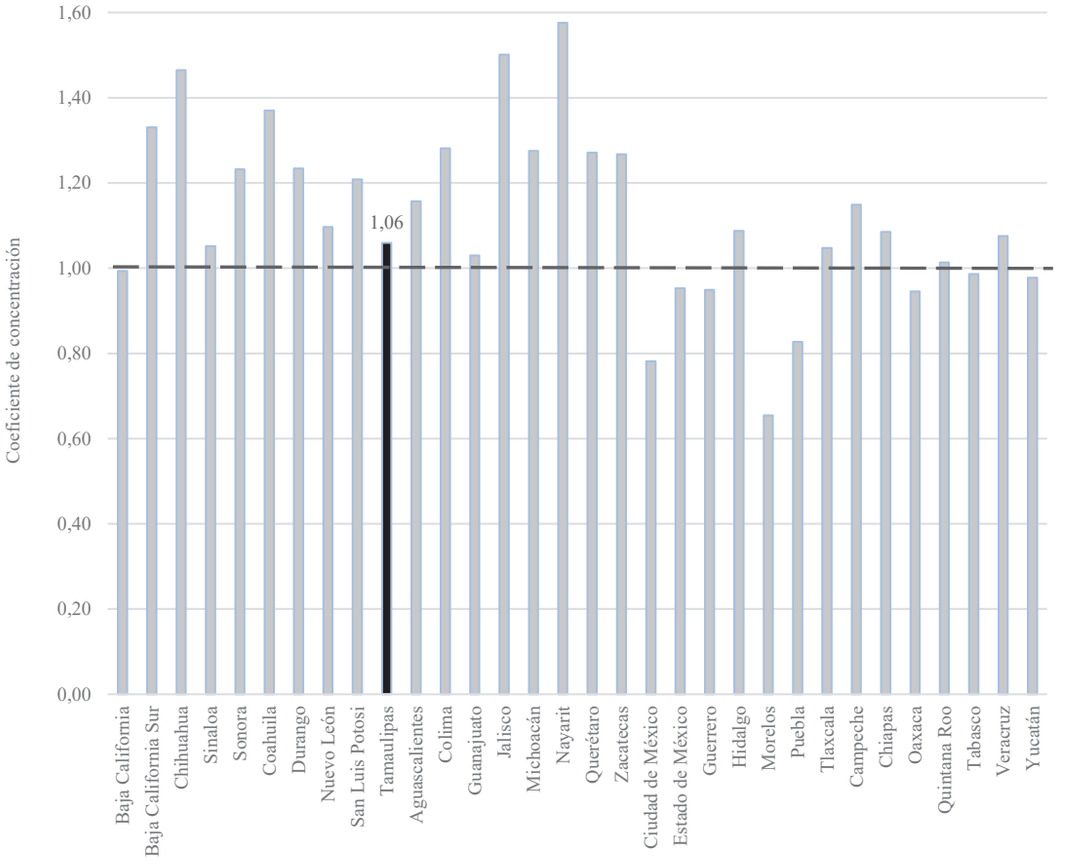

Figura 3. Coeficiente de localización del Ciberfraude al comercio electrónico en México 2019.
Fuente: Elaboración propia con información de la Policía Federal mediante solicitud pública.

PODIUM No. 41, Junio 2022, pp. 21-40

ISSN: 1390-5473 e-ISSN: 2588-0969

aquellos estados que presentan mayor cantidad de delitos poseen mecanismos particulares para hacerles frente de mejor manera. Así, dicho dato despierta interés por conocer los factores que determinan la presencia del ciberfraude al comercio electrónico en cierto espacio geográfico.

Por otro lado, el noreste del país -donde se ubica Tamaulipas- ocupó la posición cinco en compradores en línea en 2019, manifestando un porcentaje significativo de compradores (11 %) (Asociación de Internet MX, 2019a). De hecho, la entidad mostró un incremento en dicho rubro en los últimos años. En 2017, los usuarios que compraron bienes y servicios en internet fueron de 20.8 %, pero en 2020 el porcentaje aumentó a 31.6 % (Inegi, 2017, 2018, 2020), una tendencia similar a la mayoría de los estados de la República (Asociación de Internet MX, 2017), que pone en riesgo a los tamaulipecos.

Es importante destacar que los registros de la Policía Federal obtenidos están conformados por llamadas a la corporación, infiriendo que las personas físicas y morales están siendo afectadas. Este hecho coincide con lo establecido por la Condusef (s.f), al remarcar que últimamente se están presentando los ciberataques dirigidos a este grupo -y específicamente por banca móvil. Con ello las personas vulnerables (por falta de conocimientos y recursos económicos) pueden ser las potenciales víctimas (UNCATD, 2020).

Son varios los factores que inciden en el éxito del comercio electrónico como opción de negocios; uno de ellos tiene que ver con la ciberseguridad de los involucrados en tales transacciones, siendo uno de los elementos determinantes para este logro (Ríos Ruíz, 2014). Con todo, algunos autores opinan que las empresas en México son incapaces de ofrecer a sus clientes seguridad en sus movimientos financieros (Hernández Mendoza et al., 2018).

Un reflejo de esto son los obstáculos de operación que los usuarios refieren para adquirir bienes o servicios vía internet donde gran parte se relaciona con la seguridad en el pago o en el hecho de entregar datos bancarios o personales a las páginas web que lo solicitan (Inegi, 2019). Los hallazgos coinciden con lo encontrado en localidades del país -como Hermosillo, Sonora y Guadalajara, Jalisco- donde el consumidor prefiere la forma tradicional de compra. Por un lado, verificar en persona la calidad del producto, y por otro, pagar por otros medios que no involucran sus datos financieros (Bocanegra Gastélum y Vázquez Ruíz, 2008; Vargas Hernández et al., 2019).

Lo anterior muestra las debilidades que presenta el sistema comercial mexicano para adaptarse y formar parte del desarrollo digital que se espera en la sociedad actual.

Conclusiones

La compra y venta de productos y servicios a través de medios digitales son transacciones de *comercio electrónico*.

PODIUM No. 41, Junio 2022, pp. 21-40

ISSN: 1390-5473 e-ISSN: 2588-0969

Existe consenso en las posibilidades mercantiles que ofrece esta actividad a los vendedores, reconociendo las ventajas y comodidades de esta modalidad para los consumidores. Sin embargo, su expansión a través de canales no presenciales se ha acompañado de casos de fraude electrónico.

En esta investigación se constató que existe concentración del fraude al comercio electrónico de 2018 a 2019 en tres estados de la República: Nayarit, Jalisco y Chihuahua. Dichas entidades no poseen altos niveles de actividad en este comercio, por lo que la primera hipótesis fue refutada. Las técnicas utilizadas fueron muy variadas, siendo las principales el uso de redes sociales para robar contraseñas, por correo electrónico y portales de internet falsos (*phishing*), virus o códigos maliciosos para robar datos de computadora y extorsionar (*criptolocker*).

Para el caso de Tamaulipas, existió concentración de denuncias del ciberfraude al comercio electrónico en dicho periodo. Si bien la entidad no mostró altos niveles como otros estados, sí se colocó dentro del rango señalado por el modelo de análisis aplicado, considerando que la entidad adquiere relevancia como territorio propenso a este ciberfraude en el contexto nacional. Los métodos para tal fin se alinean en parte con las tendencias actuales, más con las afectaciones a bienes patrimoniales personales. Con ello se puede establecer que Tamaulipas se ubica dentro del grupo de entidades del país que merece especial atención en la materia, por lo que será necesario indagar en los factores que inciden en su presencia y diseñar políticas públicas según resulte.

Ahora bien, la entidad aventajó a otras en el nivel de concentración de quejas, según la media nacional, sobrepasando a estados donde existen más ciberedelitos, y la compra de servicios y productos es mayormente activa. Por lo tanto, la hipótesis establecida como primera se refuta. En ese sentido, se recomienda realizar estudios que aborden los determinantes de los ciberdelitos en un lugar en particular. En el Tamaulipas, conviene analizar a cuánto ascienden las pérdidas monetarias por este fraude y qué sectores y municipios son los más afectados, para diseñar soluciones focalizadas que atiendan la problemática.

Por lo tanto, se puede establecer que el contexto es un elemento importante para el diseño de iniciativas y la puesta en marcha de acciones de política pública que inhiban las prácticas digitales delictivas en Tamaulipas, pues las tendencias de fraude en la compraventa en línea limitan el crecimiento económico de la entidad, y en consecuencia del país. Así, en Tamaulipas faltaría aprovechar las ventajas del comercio electrónico, estableciendo condiciones que permitan a los usuarios realizar transacciones electrónicas con reducción de riesgo.

Además, el ciberfraude es una actividad ilícita cotidiana que genera grandes pérdidas económicas, originando otras problemáticas donde no solo los bienes materiales y económicos se ven

PODIUM No. 41, Junio 2022, pp. 21-40

ISSN: 1390-5473 e-ISSN: 2588-0969

afectados, sino que provoca inestabilidad económica y social, y altera la paz en la sociedad debido a la inseguridad virtual. Es importante mencionar que la atención de tales delitos en México corresponde a la Unidad de Ciberseguridad, adscrita a la División Científica de la Policía Federal, y desde donde se realizan acciones de prevención e investigación de conductas ilícitas a través de medios informáticos. A su vez, esta instancia alberga el Centro Nacional de Respuesta a Incidentes Cibernéticos de la Policía Federal (CERT-MX) encargado de prevenir y mitigar las amenazas de seguridad informática que ponen en riesgo la infraestructura tecnológica y la operatividad del país (Policía Federal, 17 de mayo de 2018).

Si la pandemia está dando paso a nuevos fenómenos relacionados con las TIC, las medidas deben orientarse a la protección de las personas cuando se convierten en usuarios asiduos de las mismas, mayormente de quienes encuentran en internet un nuevo espacio de emancipación económica. Así, los gobiernos de México y Tamaulipas deberán ajustarse a las dinámicas que tienen que ver con el comercio electrónico para que sea un pilar fundamental de la economía. Fomentar que las empresas mexicanas utilicen herramientas digitales para su crecimiento y competitividad. Así mismo, proveer a los ciudadanos de los recursos (económicos y financieros), habilidades y capacidades para comerciar de esta manera. Por otro lado, generar mecanismos vinculantes con instituciones financieras para mejorar la ciberseguridad implementadas y su actualización de acuerdo con el avance del cibercrimen y arrojen resultados.

Será crucial fortalecer el marco legislativo y establecer medidas de seguridad en el comercio electrónico que dé certeza de seguridad personal y financiera a clientes y empresas. Instando a colaborar con dependencias como el Instituto Federal de Telecomunicaciones (IFT), el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), Policía Federal y la Secretaría de Economía, para homologar criterios tipológicos que permitan intercambio de información y combatir estos delitos desde sus respectivas atribuciones (Condusef, 2018). Que será fundamental para enfrentar los factores asociados al crecimiento del comercio electrónico; no sin asegurar que los demás elementos de la agenda digital (contenidos y capacidades) estén garantizados en México para eliminar la brecha digital que todavía persiste. Mismo caso si se quiere migrar a una sociedad de la información y del conocimiento.

Contribución de autores

R.A.D.A. Revisión de literatura, metodología, análisis de datos, discusión y conclusiones, y revisión de redacción.

R.V.V. Revisión de literatura, metodología, análisis de datos, discusión y conclusiones, y revisión de redacción.

Referencias

Acosta, M. G., Benavides, M. M., y García, N. P.

PODIUM No. 41, Junio 2022, pp. 21-40

ISSN: 1390-5473 e-ISSN: 2588-0969

(2020). Delitos informáticos: Impunidad organizacional y su complejidad en el mundo de los negocios. *Revista Venezolana de Gerencia 2020, 25(*89), 18-22.

Álvarez, F. (2020). Machine Learning en la detección de fraudes de comercio electrónico aplicado a los servicios bancarios. *Ciencia y Tecnología,* (20), 81-95.

Arsene, L. (2020). Coronavirus-themed Threat Reports Haven't Flattened The Curve. *Bitdefender Labs teams*. https://labs.bitdefender.com/2020/04/coronavirus-themed-threat-reports-havent-flattened-the-curve/

Asociación de Internet MX. (2017). *Estudio de Comercio Electrónico en México 2017*. https://irp-cdn.multiscreensite.com/81280eda/files/uploaded/Estudio%20de%20Comercio%20Electr%C3%B3nico%202017.pdf

Asociación de Internet MX (2019a). *15°Estudio sobre los Hábitos de los Usuarios de Internet en México 2018*. Movilidad en el Usuario de Internet Mexicano. https://irp-cdn.multiscreensite.com/81280eda/files/uploaded/15%2BEstudio%2Bsobre%2Blos%2BHa_bitos%2Bde%2Blos%2BUsuarios%2Bde%2BInternet%2Ben%2BMe_xico%2B2019%2Bversio_n%2Bpu_blica.pdf

Asociación de Internet MX (2019b). *Estudio sobre Comercio Electrónico en México 2019 (décima tercera entrega)*. Estadística Digital. https://irp-cdn.multiscreensite.com/81280eda/files/uploaded/Estudio%20de%20Comercio%20Electro%CC%81nico%20en%20Me%CC%81xico%202019.pdf

Avendaño, O. (2018). Los retos de la banca digital en México. *Revista IUS, 12* (41), 87-108.

Banco Interamericano de Desarrollo [BID] y Organización de los Estados Americanos [OEA]. (2020). *Ciberseguridad riesgos, avances y el camino a seguir en América Latina y El Caribe*: Reporte Ciberseguridad 2020. https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf

Bocanegra Gastélum, C. y Vázquez Ruíz, M. (2008). Comercio electrónico en una localidad de México. *Comercio Exterior, 58*(11), 788-793.

Cámara Colombiana de Informática y Telecomunicaciones – CCIT. (2019). Tendencias cibercrimen Colombia 2019 – 2020. https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf

Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros -Condusef. (s.f.). 3.3 millones de reclamaciones por fraude se registran en el primer semestre del año. https://www.condusef.gob.mx/?p=contenido&idc=448&idcat=1

Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros -Condusef. (2018). Portal de Fraudes Financieros en México. Octubre de 2018. https://www.condusef.gob.mx/documentos/prensa/400983_PORTAL_DE_FRAUDES_FINANCIEROS_vers7.pdf

Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros -Condusef. (2019). ¡Aguas con los fraudes! Blog. https://www.gob.mx/condusef/articulos/aguas-con-los-fraudes

Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros -Condusef. (2021a). CONDUSEF atendió 1,672 controversias en el estado de Tamaulipas durante enero mayo de 2021. https://www.condusef.gob.mx/index.php/documentos/estadistica/estad2021/reclamacionesporsectorfinanciero2021.pdf?p=contenido&idc=1726&idcat=1

Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros -Condusef. (2021b). Portal de fraudes financieros. Monitor de reportes. Búsqueda de posibles datos fraudulentos. https://phpapps.condusef.gob.mx/fraudes_financieros/monitor.php?id=5&r=10303

eComerce Institute. (2012). Fraude comercio electrónico en Latinoamérica. https://ecommerce.institute/fraude-comercio-electronico-en-latinoamerica/

PODIUM No. 41, Junio 2022, pp. 21-40

ISSN: 1390-5473 e-ISSN: 2588-0969

Estupiñán Gaitán, R. (2002). *Control interno y fraudes*. ECOE ediciones..9630.

González García, J. (2020). Comercio electrónico en China y México: surgimiento, evolución y perspectivas. *México y la Cuenca del Pacífico, 9* (27), 53-84.

Hernández, A. (13 de julio de 2018). Al mes, hasta 300 denuncias por delitos cibernéticos: ciberacoso, bullying, sexting y robo de identidad. *Milenio*. https://www.pressreader.com/

Hernández, A. (31 de marzo de 2021). Policía de Tamaulipas recibe 2 mil 300 denuncias por delitos cibernéticos. *Milenio*. https://www.milenio.com/policia/tamaulipas-policia-recibe-2-mil-300-denuncias-delitos-internet

Hernández Mendoza, S., Olguín Guzmán, E., y Hernández Mendoza, J. (2018). Comercio electrónico como herramienta complementaria en las PYMEs en México. *Etic@net: Revista científica electrónica de Educación y Comunicación en la Sociedad del Conocimiento, 18*(2), 245-273.

Instituto Nacional de Estadística y Geografía – Inegi. (2015). Módulo sobre Ciberacoso (Mociba). Principales resultados. https://www.inegi.org.mx/contenidos/investigacion/ciberacoso/2015/doc/mociba2015_resultados. pdf

Instituto Nacional de Estadística y Geografía-Inegi. (2017). Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares (ENDUTIH), 2017. Usuarios de Internet por entidad federativa, según principales usos, 2017. https://www.inegi.org.mx/programas/dutih/2017/

Instituto Nacional de Estadística y Geografía-Inegi. (2018). Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares (ENDUTIH), 2018. Usuarios de Internet por entidad federativa, según principales usos, 2018. https://www.inegi.org.mx/programas/dutih/2018/

Instituto Nacional de Estadística y Geografía-Inegi. (2019). Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares (ENDUTIH), 2019. https://www.inegi.org.mx/programas/dutih/2019/

Instituto Nacional de Estadística y Geografía-Inegi. 2020. Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares (ENDUTIH), 2020. Usuarios de Internet por entidad federativa, según principales usos, 2020. https://www.inegi.org.mx/programas/dutih/2020/

Instituto Nacional de Estadística y Geografía-Inegi. (2021). Encuesta Nacional de Ocupación y Empleo (ENOE) 2005-2021. https://www.ipade.mx/wp-content/uploads/2017/04/Estadisticas_sobre_mujeres_y_empresarias_en_Mexico.pdf

Isard, W. (1962). Methods of Regional Analysis: an Introduction to Regional Science. *Cambridge, Massachusetts: MIT Press.*

Lara Guijarro, E.G. y Albán Silva, L.C. (2017). Los riesgos de las transacciones bancarias por Internet. *Revista Publicando, 4(*10), 62-74.

McKinsey & Company, Consejo Mexicano de Asuntos Internacionales-Comexi. (2018). *Perspectiva de ciberseguridad en México.* https://consejomexicano.org/multimedia/1528987628-817.pdf

Naciones Unidas (2015). Prevenir la criminalidad, clave para el desarrollo sostenible. https://www.un.org/es/events/crimecongress2015/

Notimex (26 de enero de 2020). Quejas por fraudes cibernéticos aumentaron .38% en el 3T del 2019: Condusef. *El economista*. https://www.eleconomista.com.mx/sectorfinanciero/Quejas-por-fraudes-ciberneticos-aumentaron-38-en-el-3T-del-2019-Condusef-20200126-0028.html

Organización de los Estados Americanos – OEA. (2019). *Estado de la ciberseguridad en el sistema financiero mexicano*. Programa de Ciberseguridad del Comité Interamericano contra el Terrorismo de la Organización de los Estados

PODIUM No. 41, Junio 2022, pp. 21-40

ISSN: 1390-5473 e-ISSN: 2588-0969

Americanos. https://www.oas.org/es/sms/cicte/documents/informes/Estado-de-la-Ciberseguridad-en-el-Sistema-Financiero-Mexicano.pdf

Organización Mundial del Comercio -OMC. (2021). Entender la OMC: cuestiones transversales y cuestiones nuevas. https://www.wto.org/spanish/thewto_s/whatis_s/tif_s/tif_s.htm

Oxman, N. (2013). Estafas informáticas a través de Internet: acerca de la imputación penal del "phishing" y el "pharming". *Revista de Derecho de la Pontificia Universidad Católica de Valparaíso*, (41), 211-262.

Paz Sefair, A. (2018). La culpa del consumidor en la responsabilidad financiera y su proyección causal en el daño por fraude electrónico. Una mirada a la jurisprudencia de la Delegatura para Funciones Jurisdiccionales de la Superintendencia Financiera de Colombia. *Revista de Derecho Privado*, (35), 261-289.

Pecoy Taque, M. (2011). Delito en el comercio electrónico. *Prisma Jurídico, 10* (1), 209-224.

Peñaloza, M. C., y Morillo, M. C. (2010). El sector servicios y los delitos informáticos. *Visión Gerencial*, (2), 358-370.

Policía Federal (17 de mayo de 2018). *Centro Nacional de Respuesta a Incidentes Cibernéticos de la Policía Federal*. Gobierno de México. https://www.gob.mx/policiafederal/articulos/centro-nacional-de-respuesta-a-incidentes-ciberneticos-de-la-policia-federal?idiom=es

Quevedo González, J. (2017) *Investigación y prueba del ciberdelito* [Tesis de doctorado, Universidad de Barcelona]. http://hdl.handle.net/10803/665611

Ríos Ruíz, A. (2014). Análisis y perspectivas del comercio electrónico en México. Enl@ce Revista Venezolana de Información, Tecnología y Conocimiento, 11(1), 97-121.

Rufín Moreno, R. (2002). Comercio electrónico de las empresas turísticas: la función de las entidades financieras respecto a la seguridad en el pago. *Estudios Turísticos*, (153), 3-17.

Sánchez Salinas, O. (2014). *Análisis espacial del delito: la relación entre el delito y las características sociodemográficas en las delegaciones Benito Juárez, Coyoacán y Cuauhtémoc del D.F. 2010.* [Tesis de Maestría, El Colegio de la Frontera Norte].

Sanz Párraga, F. (2016). *Fraudes en Internet* [Tesis de Grado, Universitat Jaume] http://repositori.uji.es/xmlui/bitstream/handle/10234/161482/TFG_2015_SanzP%C3%A1rragaF.pdf?sequence=1

Symantec. (2019) *Internet Security Threat Report, 24.* http://latixns.mx/wp-content/uploads/2019/03/Internet-Security-Threat-Report-20190314.pdf

Téllez, J. (1996). Los delitos informáticos: situación en México. *Informática y derecho: Revista iberoamericana de derecho informático, 1*(9), 461-474.

United Nations Conference on trade development -UNCTAD. (2020). The UNCTAD B2C E-commerce Index 2020: Spotlight on Latin America and the Caribbean. UNCTAD Technical Notes on ICT for Development No. 17. 17 Feb 2021. https://unctad.org/es/node/32189

Vargas Hernández, J., Vázquez Ávila, G. y Vargas Chew, A. (2019). Una aproximación al comercio electrónico en Guadalajara (México). *Investigación y Marketing*, (144), 44-52.

PODIUM No. 41, Junio 2022, pp. 21-40

ISSN: 1390-5473 e-ISSN: 2588-0969