UNIVERSIDAD NACIONAL AUTÓNOMA DE NICARAGUA

FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES

MONOGRAFÍA

Para optar al título de:

Licenciado en Derecho

Análisis jurídico de las transacciones electrónicas frente a los diferentes tipos de fraude en los establecimientos comerciales del centro de la ciudad de León, Nicaragua en el año 2021.

Autores:

Br. Tomas Eduardo Berrios Guevara

Br. Cristhian Alexander Chavarría Poveda

Tutor:

M.Sc. Asdrúbal René Sotelo Niño

Septiembre del 2022.

Agradecimientos

A Dios, a mi Familia por apoyarme en cada momento, a mis maestros por cada consejo y enseñanza y cada persona que estuvo conmigo.

Berrios Guevara, Tomas Eduardo

A Dios, a cada uno de mis seres queridos por apoyarme en cada paso que he dado, a mis maestros por guiarme con sus enseñanzas.

Chavarría Poveda, Cristhian Alexander

Resumen

La investigación de las transacciones electrónicas frente a los diferentes tipos de fraude plantea un estudio a una nueva problemática que ha surgido recientemente, es por ello que la investigación fue de tipo mixto, ya que se emplearon métodos cuantitativo y cualitativo, para un estudio más completo y detallado, se recopilaron datos de fuentes documentales tales como leyes, libros, tesis, artículos científicos y/o cualquier otro tipo de documento gráfico, icnográfico y electrónico en su mayoría[1]. De igual forma, se recopilaron y analizaron datos a través de encuestas. En el mismo sentido, se utilizó un método de análisis síntesis[2]**,** donde se realizó una separación de la parte de un todo con la finalidad de estudiarlas en forma individual para después efectuar la reunión racional de los elementos dispersos y analizarlos en su totalidad. De la misma manera, el método comparativo se utilizó para analizar las particularidades del sujeto de estudio en relación con otros siguiendo este método de investigación, tanto el planteamiento del problema, la forma y las técnicas de recopilar datos, como el análisis y la explicación de sus resultados estuvieron encaminados hacia un mejor entendimiento del comportamiento del fenómeno que se estudió[3], la presente investigación es de corte transversal dado que fue una investigación observacional que analizó datos de variables recopiladas en un periodo de tiempo sobre una población muestra o subconjunto predefinido. Además, se empleó el método deductivo**,** sabiendo que se partió del marco general de cómo funcionan las transacciones electrónicas, así como también el análisis jurídico de las mismas y el tratamiento que se debe de tener cuando se enfrente a los diferentes tipos de fraudes con la finalidad de poder detectarlos antes que logren hacer algún daño y hacia lo particular cómo funcionan realmente las transacciones electrónicas en la sociedad.

[1] MUÑOZ RAZO, Carlos. *Como elaborar y asesorar una investigación de tesis*, 2da Ed. México, Pearson Educación, 2011, p.14.
[2] VILLABELLA ARMENGOL, Carlos. *La investigación y comunicación científica en la ciencia jurídica*, 1ra Ed. México, Instituto Mexicano de Ciencias Jurídicas de Puebla, 2009, p.37
[3] MUÑOZ RAZO, Carlos, *op.cit.*, p.23

León, 21 de septiembre de 2022.

M.Sc. Ximel Castellón.
Jefa Departamento de Administración y Políticas Públicas.
Facultad de Ciencias Jurídicas y Sociales.
UNAN – León
S.D.

Estimada profesora:

Reciba saludos cordiales de mi parte. Es mi deseo que siga cosechando éxitos en este año 2022, La presente tiene por objeto hacer de su conocimiento que la tesis denominada **"Análisis Jurídico de las transacciones electrónicas frente a los diferentes tipos de fraude en los establecimientos comerciales del centro de la ciudad de León, Nicaragua en el año 2021." Elaborada por los bachilleres: Tomas Eduardo Berrios Guevara, Cristhian Alexander Chavarría Poveda.**

Ha sido concluida de manera satisfactoria, y cumple con los requisitos establecidos en los artículos del 41 al 79 del Reglamento de Formas de Finalización de los Estudios, en tal sentido estoy autorizando la misma en mi calidad de tutor, para que los anteriormente mencionados bachilleres puedan ejercer su Derecho a la defensa.

Agradezco la atención a la presente.

_____

M.Sc. Asdrúbal René Sotelo Niño.
Académico Departamento de Administración y Políticas Públicas
Facultad CCJJ y SS

cc. Archivo.

Índice

Introducción 1

Objetivos 3

Capítulo I: Consideraciones Generales sobre el Comercio Electrónico y Las Diferentes Transacciones Electrónicas Que Se Realizan En El Municipio De León, Nicaragua. 4

1. Del trueque al comercio electrónico, surgimiento y evolución del comercio. 4

1.1 El papel del Internet en el desarrollo comercial 6

1.2 El comercio electrónico (*E-commerce*) 7

1.3 Pandemia COVID-19 y su impacto en el comercio electrónico 10

1.4 El futuro del comercio electrónico, la web 3.0 y las criptomonedas 11

1.5 Las Criptomonedas 12

2. Diferentes transacciones electrónicas que se realizan en el municipio de León departamento de León, Nicaragua 13

Capítulo II: Marco jurídico regulador de las transacciones electrónicas en Nicaragua 21

2.1 En la Constitución Política de Nicaragua 21

2.2 Ley Especial de ciberdelitos 21

2.3 Ley De Protección De Los Derechos De Las Personas Consumidoras Y Usuarias 23

2.4 Ley General de Telecomunicaciones y Servicios Postales 24

2.5 Ley General De Bancos Y Otras Instituciones Financieras y Norma sobre Gestión de Riesgo Tecnológico SIBOIF 25

2.6 Comparación entre leyes internacionales y la legislación nicaragüense 26

2.6.1 Ley Gramm-Leach-Bliley 26

2.6.2 Ley Federal De Protección Al Consumidor México 27

2.7 Derecho Informático 28

Capítulo III: Tipos de fraude que se presentan en las transacciones electrónicas en los establecimientos comerciales del municipio de León, Nicaragua 34

3.1 Tipos de Fraudes en Nicaragua 34

3.2 Unidad de Análisis Financiero 46

Diseño Metodológico 48

Conclusiones 51

Recomendaciones 52

Fuentes del conocimiento 53

Anexo 57

Introducción

Los avances tecnológicos que trajo consigo siglo veinte y parte del veintiuno han logrado que el comercio electrónico se desarrolle exponencialmente, dicho tipo de comercio se vuelto más práctico gracias al acceso que se tiene hoy en día a la tecnología. Para realizar una transacción o para establecer un comercio electrónico, basta con conectarse a la red y usar una de las diferentes plataformas existentes, la rapidez y facilidad con que se realizan estas operaciones a través de Internet son las razones por las cuales se han vuelto tan populares hoy en día. Esta herramienta de comercio se volvió aún más necesaria durante la pandemia del SARS-CoV-2(COVID-19), dado que facilita el comercio, estas transacciones electrónicas permiten que las compras o ventas se realicen desde cualquier lugar y en cualquier momento, sin la necesidad de la presencia física.La problemática de este tipo de comercio se encuentra en sus mismas ventajas, debido a que su fácil acceso es usado muchas veces por terceras personas para cometer operaciones maliciosas u obtener datos personales o financieros, esta figura es conocida fraude electrónico.

En Nicaragua el comercio electrónico es relativamente nuevo, debido a esto, tanto su regulación como la seguridad de los consumidores al hacer uso de esta herramienta es uno de los principales problemas que afecta al sistema mercantil nicaragüense, dado que este se encuentra frágil ante las diferentes formas de fraude electrónico por lo que no existen suficientes leyes o instituciones encargadas de su regulación.

Se procuró realizar un análisis doctrinario y normativo de las transacciones electrónicas, colocándolas como figuras que van siendo parte el día a día de las personas consumidoras y las empresas en general, las cuales se han encontrado vulnerables antes los tipos de fraudes que poco a poco van surgiendo en nuestro país.

Por tal motivo, en el primer capítulo se puedeobservar un recorrido histórico y evolutivo de las transacciones, comenzando con el trueque hasta la actual forma de comercio electrónico, donde se ven aquellos aspectos generales del impacto de la globalización en el desarrollo del comercio internacional. A su vez, se el surgimiento de la Organización Mundial del Comercio

(OMC) como principal institución que rige al comercio y como el *internet* es el principal motor para el desarrollo del comercio electrónico.

De igual forma, se aborda el impacto de la pandemia del Covid-19 en el comercio electrónico y como este impulso el uso y crecimiento a nivel mundial de las transacciones electrónicas, así mismo abarcamos el surgimiento de las monedas electrónicas como nuevas formas de comerciar en el mundo de los *E-commerce* y el futuro del Comercio electrónico.

Siguiendo, en el segundo capítulo de esta investigación se encontrará el marco jurídico que regulan las transacciones electrónicas en Nicaragua, partiendo desde lo establecido en la Constitución Política de nuestro país en donde se regulan las actividades económicas. Así también, la Ley de Protección de Los Derechos de las Personas Consumidoras y Usuarias donde se trata de garantizar y promover el consumo responsable para que las personas -ya sea jurídicas o naturales- que utilizan los medios electrónicos como una plataforma de mercado digital se sientan seguros sobre la veracidad y la calidad de bienes y servicios.

Por otro lado, se incluye la Ley General De Bancos Y Otras Instituciones Financieras para mostrar como mediante la Superintendencia de Bancos y Otras Instituciones Financieras (SIBOIF) y su norma de gestión de riesgo donde se regula el funcionamiento de todos los bancos, sucursales y agencias bancarias que operan en Nicaragua. También se abarca derecho comparado al analizar leyes extranjeras como la Ley Gramm-Leach-Bliley de Estados Unidos de América y la Ley Federal De Protección al Consumidor de México que tienen relación con leyes de nuestro ordenamiento jurídico nicaragüense. por último, se describe los aspectos generales del Derecho Informático y su incidencia en el comercio electrónico dada a su reciente aparición en los cuerpos normativos.

Finalmente, en el tercer capítulo, se exponen los diferentes tipos de fraudesen las transacciones electrónicas que se logró identificar en nuestro estudio. Por último, se plasmó un estudio realizado por la Unidad de Análisis Financiero de Nicaragua (UAF) donde se aborda el aumento de los fraudes de aprovechados por el aumento del uso de las plataformas electrónicas debido a la pandemia del COVID-19.

Objetivos

Objetivo general

Analizar jurídicamente las transacciones electrónicas frente a los diferentes tipos de fraude en el municipio de León, departamento de León, Nicaragua.

Objetivos específicos

- Determinar las diferentes transacciones electrónicas que se realizan el municipio de León, departamento de León en León, Nicaragua;
- Analizar el marco jurídico regulador de las transacciones electrónicas en Nicaragua;
- Identificar los tipos de fraudes que se presentan en las transacciones electrónicas el municipio de León, departamento de León en León, Nicaragua.

Capítulo I: Consideraciones Generales sobre el Comercio Electrónico y Las Diferentes Transacciones Electrónicas Que Se Realizan En El Municipio De León, Nicaragua.

1. Del trueque al comercio electrónico, surgimiento y evolución del comercio.

Referirse al comercio electrónico es referirseauna forma de comercio que durante la última década ha tenido un desarrollo impredecible gracias a diversos factores que han propiciado su aceleración. Primeramente, se abordará al comercio como tal y luego su evolución a través del tiempo. La palabra comercio proviene del latín *commercĭum*, que significa 'compra y venta de mercancía'. El comercio es definido por Cabanellas como la negociación o actividad que busca la obtención de ganancias o lucro en la venta, permuta o compra de mercadería[4]. También se puede definir al comercio como el conjunto de negociaciones que forman parte de dicho proceso. El primer indicio de lo que hoy se conoce como comercio empezó con eltrueque[5] que fue la manera en que las antiguas civilizaciones empezaron a comerciar, esta forma de comercio surge como manera de obtener alimentos o utensilios, este sistema no concibe afianzarse en el mercado por la dificultad deque ambas partes debían estar interesadas en los productos a intercambiar, otro obstáculo es que debían llegar a un acuerdo en cuanto al valor que tenían dichos objetos para que el cambio fuese equitativo.

Este problema es solucionado con el surgimiento de la moneda o dinero[6] alrededor de los años 700 y 500 A.C. La moneda revoluciona la manera de comerciar dejando atrás al trueque, la moneda se concibió como un medio acordado en la sociedad para el intercambio de mercancías y bienes, logrando estandarizar el concepto del valor y simplificando el comercio. El dinero revolucionó el comercio como una nueva forma de unidad de cuenta y una herramienta para almacenar valor, ya que fue posible contar las monedas en lugar de pasarles, lo cual facilitó las transacciones comerciales y abrió paso al comercio internacional, estosignificó un gran avance en la economía y el mercado.

[4]CABANELLAS, Guillermo, *Diccionario jurídico elemental*, duodécima edición, editorial Heliasta, 1998, p.76.
[5]El trueque es el intercambio de bienes o servicios entre dos o más personas a cambio de otros bienes o servicios sin necesidad de que exista ningún tipo de dinero por medio.
[6]Históricamente ha habido muchos tipos diferentes de moneda, desde cerdos, dientes de ballena, cacao, o determinados tipos de conchas marinas. Sin embargo, el más extendido sin duda a lo largo de la historia es el oro.

Ya establecidos en la edad media, surgieron rutas comerciales transcontinentales que intentaban suplir la alta demanda de bienes y mercancías europeas siendo la famosa ruta de la seda, pero también había otras importantes como las rutas de importación de pimienta, de sal o de tintes, esto significo el desarrollo y expansión del comercio europeo y asiático, trayendo consigo un desarrollo comercial más integrado gracias a la moneda.

Cerca del año 1400, la disrupción del Imperio Mongol, el crecimiento del Imperio otomano y el fin del Imperio bizantino provoca que todas las rutas de comercio europeas con el Este queden bloqueadas. Es gracias a esto que, surge la búsqueda de nuevas rutas de comercio, lairrupción del capitalismo mercante y el deseo de explorar el potencial de una economía global impulsó en Europa la era de los descubrimientos. Fue así como Europa se volcó en la búsqueda de nuevas rutas hacia la India con el fin de restablecer la importación de especias[7].

Fue el descubrimiento de América por los europeos el cual supuso otro paso en el comercio. Portugal y España fueron los dos países que obtuvieron el monopolio de estas rutas, el nuevo flujo de oro que obtenían los españoles de manera casi gratuita en América saneó y consolidó el mercado comercial y de capital europeo[8].

El nacimiento de la Revolución Industrial en Inglaterra, la evolución del comercio internacional yel apoyo de la industria mecánica, el comercio alcanzó un florecimiento extraordinario. Las operaciones bursátiles aumentaron durante esta época y ya para el sigloXIX, el capitalismo[9] reflejó importantes cambios en la estructura material del comercio internacional, también se unificó el capital bancario y apareció el capital financiero.

[7]Historia del Comercio Internacional - Grupo Codecominter - Agente de Aduanas y Abogados y Notarios. *Grupo Codecominter - Agente de Aduanas y Abogados y Notarios* [en línea], 2021. [Consulta: 5 junio 2022].https://www.codecominter.com/historia-del-comercio-internacional/

[8] . (SITIO, M., 2022. Historia - MI SITIO WEB G.S. Google.com [en línea]. [Consulta: 5 junio 2022]. Disponible en: https://sites.google.com/site/misitiowebgs/comercio/historia.

[9]El capitalismo es el sistema económico que se instituyó en Europa entre los siglos XVIII y XIX. El fundamento del capitalismo es el establecimiento de compañías especializadas en la compra, producción y venta de bienes y servicios, en un mercado libre del control del Estado. La única regla que rige en un sistema capitalista puro es la ley de la oferta y la demanda.

La globalización económica[10], nació como consecuencia de la necesidad de rebajar costos de producción con el fin de dar la habilidad al productor de ser competitivo en un entorno global, el comercio internacional comienza a evolucionar[11].

Con el surgimiento de la Organización Mundial del Comercio[12]destaca la Declaración sobre el Comercio Electrónico Mundial adoptada en la Segunda Conferencia Ministerial, celebrada en mayo de 1998, en la cual se establecía un programa de trabajo amplio para examinar todas las cuestiones relacionadas con el comercio electrónico mundial que afectan al comercio, incluidas las identificadas por los Miembros. El programa de trabajo, en el que participarían los órganos competentes de la Organización Mundial del Comercio, tendría en cuenta las necesidades económicas, financieras y de desarrollo de los países en desarrollo. Debido a diferentes factores dicha declaración no obtuvo mayor alcance quedando solamente en un proyecto[13].

Entrado el siglo XX, el exponencial crecimiento del comercio internacional puede atribuirse a los diversos tratados, pactos y convenios que se solidificaron entre los países industrializados durante la segunda mitad de este siglo. Las claves de este desarrollo son gracias a los nuevos procesos de producción, los avances tecnológicos y el aumento de la población, es en esta etapa del comercio donde aparece el internet.

1.1 El papel del Internet en el desarrollo comercial

Con la creación de internet surge el concepto de *Web 1.0*[14]en esta primera etapa del internet las páginas no ofrecían funciones interactivas, los sitios web solo realizaban funciones

[10]La globalización económica es un proceso histórico, el resultado de la innovación humana y el progreso tecnológico. Se refiere a la creciente integración de las economías de todo el mundo, especialmente a través del comercio y los flujos financieros.

[11]*Ibídem.*

[12]Surgió el primero de enero de 1995, significó la mayor reforma del comercio internacional desde el final de la Segunda Guerra Mundial. Mientras que el GATT se había ocupado principalmente del comercio de mercancías, la OMC y sus Acuerdos abarcan además el comercio de servicios y la propiedad intelectual. La creación de la OMC también dio lugar a nuevos procedimientos para la solución de diferencias

[13] OMC | Comercio electrónico. Wto.org [en línea], 2022. [Consulta: 23 julio 2022]. Disponible en: https://www.wto.org/spanish/tratop_s/ecom_s/mindec1_s.htm.

[14]El término *Web* 1.0 no apareció hasta que el término Web 2.0 fue acuñado en 1999 por Darci DiNucci. Durante ese tiempo, la web estaba experimentando una gran transformación. La mayoría de los sitios web en la década de 1990

informativas. La mayoría del contenido del sitio *web* se almacenaba directamente en los archivos del sitio web, no en una base de datos separada como hoy en día. Hasta este punto hay pequeños pasos en el surgimiento del comercio electrónico, tales como *Amazon* y *eBay*.

La *web 2.0* surge gracias a la evolución de la *Web 1.0*, se caracterizópor ser una etapa más colaborativa, también es llamada la *web* de la sociedad de la información, esta etapa permitió no solo acceder a la información, sino que también colaborar o crearla, esta *web* permitió un desarrollo más significativo en la comunicación electrónica y fueron estas condiciones las cuales permitieron que el comercio electrónico encontrara su evolución, influyendo incluso en la proliferación de aplicaciones comerciales como *Amazon, Shein, Pull and Bear*, etc.. incluso la red social más utilizada en la actualidad Facebook incluyo dentro de su interfaz "*Marketplace"* una herramienta en la cual sus usuarios pueden comerciar, de igual manera la mayoría de las aplicaciones usadas hoy en día actualizaron sus interfases para ofrecer perfiles comerciales. Esta forma de comercio electrónico también podría ser llamada "Comercio electrónico informal".

Estos avances no solo beneficiaron a las grandes industrias, sino que también se nivelo un poco la balanza al proveer a los países en desarrollo grandes oportunidades en la obtención de información que antes era inaccesible. La transferencia de conocimientos resultante estimulo el crecimiento de estos países y ayudo a su integración en los mercados mundiales.

1.2 El comercio electrónico (*E-commerce*)

Elcomercio electrónico como concepto es en simples palabras compraventa o intercambio de bienes o servicios a través de medios electrónicos, pero en una definición más formal dada por la Organización Mundial del Comercio (OMC) define como: "En términos generales, es la producción, publicidad, venta y distribución de productos a través de las redes de telecomunicaciones[15]".

---

se habían creado originalmente con páginas *HTML* estáticas y algunos estilos simples incrustados en el marcado *HTML*.

[15]Concepto establecido por la Organización Mundial de Comercio, sitio web oficial, disponible en: https://www.wto.org/spanish/thewto_s/whatis_s/tif_s/bey4_s.htmconsultado el 27 de octubre de 2021.

La Organización para la Cooperación y el Desarrollo Económico lo considera así: “la venta o compra de bienes o servicios que se realiza a través de redes informáticas con métodos específicamente diseñados para recibir o colocar pedidos[16]”

Uno de los avances más significativos en el comercio electrónico fue cuando *eBay* compra *PayPal*creando así una forma más rápida y segura de enviar dinero, realizar pagos en línea, recibir dinero o configurar una cuenta de comercio, lo que facilitó las compras en comercios electrónicos.

Empieza la carrera electrónica de las empresaspor acaparar el mercado de los consumidores, en 2007*Apple* lanza al mercado el *iPhone*, y un año más tarde *Google* hace lo mismo con su versión en *Android*, ofreciendo en sus dispositivos una nueva, fácil, rápida y efectiva forma de acceder a las tiendas de *E-commerce*.

Durante los siguientes años el comercio electrónico se potencializa gracias a los avances tecnológicos, la posibilidad de tener una billetera electrónica desde tu celular, las compras en línea las cuales reducen los costos de producción.

1.2.1 Ventajas y desventajas del comercio electrónico:

Ventajas

1. Disponibilidad 24/7 los 365 días del año, es la ventaja por excelencia de esta forma de comercio;
2. Accesibilidad desde cualquier lugar, para ellosolo es necesario contar con una conexión a Internet para completar las transacciones electrónicas. Esto facilita los procesos de compra;
3. Ahorro de costes para vendedores, una tienda en línea significa menos costes de inversión y expansión a una mayor clientela;
4. Captación de clientes, las tiendas en línea te expanden a un mercado más grande;

[16]Concepto dado por la Organización para la Cooperación y el Desarrollo Económico, en el informe del Panorama del comercio electrónico, disponible en: https://www.oecd.org/sti/Panorama-del-comercio-electro%CC%81nico.pdfconsultado el 27 de octubre de 2021.

5. Recolección de datos, ofrece una interacción más personalizada con los usuarios, los consumidores dejan su rastro allá por donde pasan. Si la empresa sabe cómo gestionar los datos, puede mejorar su servicio e incluso personalizar las estrategias de marketing. Este punto es muy discutido por la violación de la privacidad de los datos.

Desventajas:

1. Inseguridad en la forma de pago, es la principal desventaja debido al miedo de los usuarios por la protección de sus datos bancarios. Las tiendas cada vez implementan sistemas más seguros para garantizar el pago con tarjetas de crédito u otros métodos;
2. Proceso de envío, existen dos desventajas la primera es el tiempo desde que se pide un producto hasta que llega al cliente depende de muchos factores. La segunda desventaja es el coste de los envíos. En ocasiones, la adquisición de un producto tiene un sobrecoste por el porte de este;
3. Mercados más competitivos, al existir mayores niveles de competitividad. Puede haber miles de tiendas con características similares. Por lo tanto, para triunfar es crucial encontrar un nicho de mercado y diferenciarse del resto de los competidores;
4. El cliente no puede probar el producto antes de comprarlo, el consumidor tiene que asumir un pequeño riesgo comprando antes de probarlo, este problema ha quedado prácticamente en el olvido, ya que la mayoría de las empresas han creado sus políticas de devolución para que si el cliente no queda satisfecho con la compra pueda devolverla sin mayor dificultad.

1.2.2 Características del comercio electrónico:

A. Mejora la competitividad y la eficiencia de las organizaciones públicas y privadas a través del abaratamiento del proceso de negociación entre clientes- usuarios y socios-proveedores;
B. El comercio electrónico es una herramienta para diversificar y penetrar en más mercados a nivel nacional e internacional;
C. Impulsa la facilitación de comercio a través de la reducción de costos transaccionales;
D. Fomenta la participación más activa de la pequeña y la mediana empresa en el comercio internacional;

E. Es una herramienta que ofrece nuevas oportunidades de desarrollo.

1.2.3 Los elementos que forman el comercio electrónico[17]:

- Involucra productos, servicios, información y pagos utilizando líneas telefónicas y redes computacionales;
- Utiliza la tecnología para la automatización del negocio y del flujo de transacciones al proveer la oportunidad de incrementar la calidad de sus productos y servicios al mismo tiempo que, incrementan la velocidad en ser entregados.

1.3 Pandemia COVID-19 y su impacto en el comercio electrónico

Con el surgimiento y rápida expansión del virus Covid-19 el *e-Commerce* presento una gran expansión, durante los primeros tres meses de 2020 las medidas sanitarias impuestas para tratar de frenar al coronavirus provocaron que millones de personas recurriesen al comercio *online*. Muchos de ellos, por primera vez.

El informe especial Digital 2020 desveló que el 47% de los internautas del mundo pasaron más tiempo realizando compras online durante la cuarentena, las razones son simples de explicar, siendo la forma óptima para obtener los productos y servicios necesarios durante el confinamiento y manteniendo el distanciamiento social, el comercio electrónico alcanzó cifras que, de otro modo, le hubiera tomado meses o años alcanzar.

El informe Digital 2022 vuelve a arrojar a la luz sobre los datos relativos a la penetración del *eCommerce* mundial, esta vez con datos relativos al 2021. Un 58,4% de la población entre 16 y 64 años compró algún producto o servicio por internet a la semana en 2021, un aumento de 11,4 puntos en relación con 2020. Esto demuestra que el éxito y uso de las tiendas online no era un efecto pasajero de la pandemia, sino una evolución natural del mercado y un canal de compra que está aquí para quedarse.

En cuanto a qué se compra en los *eCommerce*, la comida (+38%) y bebidas (+35%) son las que más crecimiento registraron, con un aproximado de USD $375.000 millones

[17] El Comercio electrónico en Centroamérica - Consortium Legal. Consortium Legal [en línea], 2020. [Consulta: 17 March 2022]. Disponible en: https://consortiumlegal.com/el-comercio-electronico-en-centroamerica/.

(poco más de 333.000 millones de euros) de gasto anual en el caso de los alimentos y USD $211.000 millones (187.000 millones de euros) en el caso de bebidas[18].

1.4 El futuro del comercio electrónico, la web 3.0 y las criptomonedas

Web 3.0 es el nombre que algunos tecnólogos le han dado a la idea de un nuevo tipo de servicio de internet en palabras de Packy McCormick, un inversionista que ayudó a popularizar la *web3.0*, la define como "una internet que es propiedad de los desarrolladores y los usuarios, coordinada con *tokens*[19]".

Los impulsores prevén que la *web3.0* adopte muchas formas, como redes sociales descentralizadas, videojuegos que recompensen a los jugadores con *tókens* criptográficos, y plataformas NFT que les permitan a las personas comprar y vender fragmentos de cultura digital. Los más idealistas afirman que la web3.0 transformará internet tal como se conoce, ya que le quitará poder a los *"gatekeepers"*, o actores tradicionales, y le dará paso a una nueva economía digital sin intermediarios.

En este escenario entra el concepto de *Blockchain* que es un sistema de almacenaje de información de manera descentralizada, con capacidad para almacenar datos con validación general, es decir, la información la introducen los usuarios y ellos mismos son quienes las verifican, lo que significa que no existen intermediarios o un sistema centralizado, es así como sedificulta que la información sea falseada porque requiere la verificación de todos los usuarios, esta red de almacenamiento de informaciónes conocida por ser la plataforma del *bitcoin* pero sus usas transciendas más allá de ello, puede usarse para firmar contratos, votar en elecciones, guardar historial médico, cadenas de suministro etc.

Esta cadena de bloques es un registro público donde están todas las operaciones de estas divisas digitales. No obstante, pese a que este sistema permite a cualquier usuario rastrear todas las transacciones hechas por todas las computadoras de la red, la información de las personas implicadas está protegida.

[18] Informe sobre la economía digital, Naciones unidas [en línea], [Consultado 23 de julio del 2022]. S.l.: Disponible en: https://unctad.org/system/files/official-document/der2021_es_0.pdf.

[19]Un token es la representación digital en el mundo *Blockchain* de algo que tiene valor dentro de un contexto. Es emitido por una entidad privada y solo es válido bajo este universo concreto. Su funcionamiento es muy similar a un plan de millas dentro de una aerolínea.

De igual forma, la seguridad de estas monedas no sólo se debe a la encriptación, sino también, a la verificación, pues el resto de los usuarios validan que la transacción pueda ser realizada de manera correcta.

1.5 Las Criptomonedas

"La relación entre el comercio digital y las criptomonedas es natural. Ambas industrias coexisten dentro del mismo marco, que se basa en brindar a los consumidores soluciones que el comercio y las finanzas tradicionales no pueden lograr" Andrew Brough, Business Development and Strategic Partnerships en CoinPayments.

Las *criptomonedas* son monedas digitales utilizadas para el intercambio de bienes o servicios. Fueron creadas a raíz de la crisis financiera del 2008 para transacciones en internet; sin embargo, en la actualidad, no sólo empresas electrónicas han aceptado criptodivisas como formas de pago, sino algunas compañías como *Starbucks, Burger King* Alemania, *Reeds Jewelers, Virgin Galactic*, entre otras, también lo hacen por sus beneficios[20].

Ya que no requieren de un administrador, es decir, no depende de los gobiernos, ni bancos, ni de ninguna institución para funcionar, permite independencia de las recesiones y crisis económicas obteniendo así la mayor cotización del mercado hasta ahora. Conjuntamente, depender de los bancos y gobiernos resulta costoso para la sociedad, debido a dos razones principales: la primera es que en los bancos estos sistemas transaccionales son muy costosos, por lo que al tener criptodivisas se reducen las comisiones y se eliminan los intereses de las operaciones realizadas; y, en segundo lugar, el gobierno no puede distorsionar las cuentas imprimiendo más dinero causando así una inflación[21].

Dentro de sus desventajas es que las divisas digitales están basadas en la especulación; por lo que no se debe interpretar como una forma de inversión sino más bien como una apuesta, apuesta que ha beneficiados más a unos que a otros.

[20]RAMÍREZ, M., 2021. Las criptomonedas y su relación con la economía mundial. Transferencia Tec [en línea]. [Consulta: 14 agosto 2022]. Disponible en: https://transferencia.tec.mx/2021/02/27/las-criptomonedas-y-su-relacion-con-la-economia-mundial/.
[21]*Ídem.*

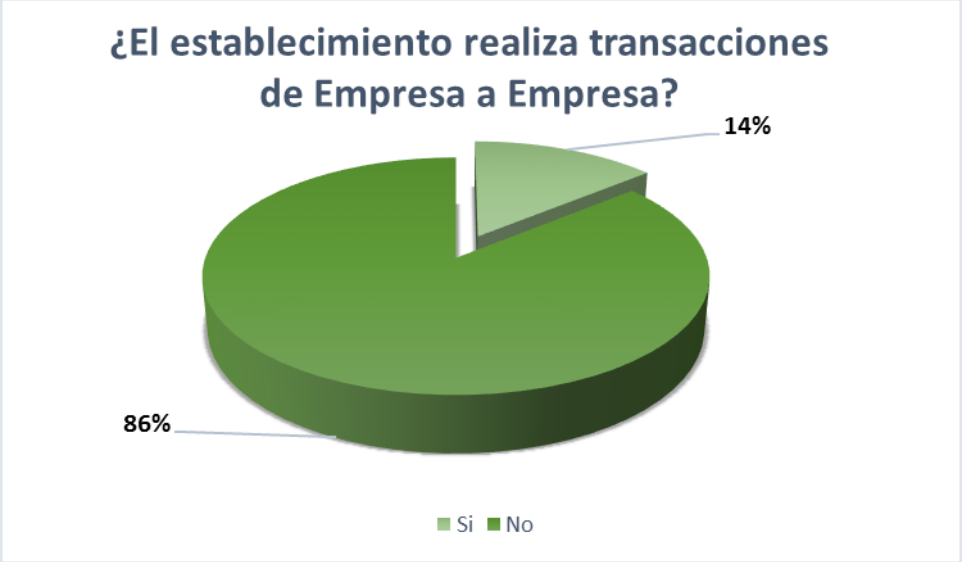
Las criptomonedas, como se puede observar, tienen una gran volatilidad especialmente en el último año. El desafío que se le presenta ahora mismo a los gobiernos es la falta de regulación fiscal de las monedas virtuales ya que en muchos países hace que exista un "vacío legal".

2. Diferentes transacciones electrónicas que se realizan en el municipio de León departamento de León, Nicaragua [22].

En esta etapa la investigaciónrefleja los resultados obtenidos en las encuestas realizadas a los establecimientos comerciales de la periferia del centro del municipio de León departamento de León, Nicaragua.Con el fin de conocercuáles son los tipos transacciones usadas en el comercio electrónico y otros datos de interés que se muestran a continuación.

1) B2B - Business to Business: Empresa a Empresa hace referencia a las operaciones comerciales que se realizan de negocio a negocio.

Grafico 5.



Fuente: Elaboracion Propia. Establecimientos comerciales del centro de la ciudad de León, departamento de León.

Conforme a la gráfica de pastel que se presenta podemos observar que el 14% de la población encuestada afirma no realizar operaciones comerciales entre empresas. Este dato

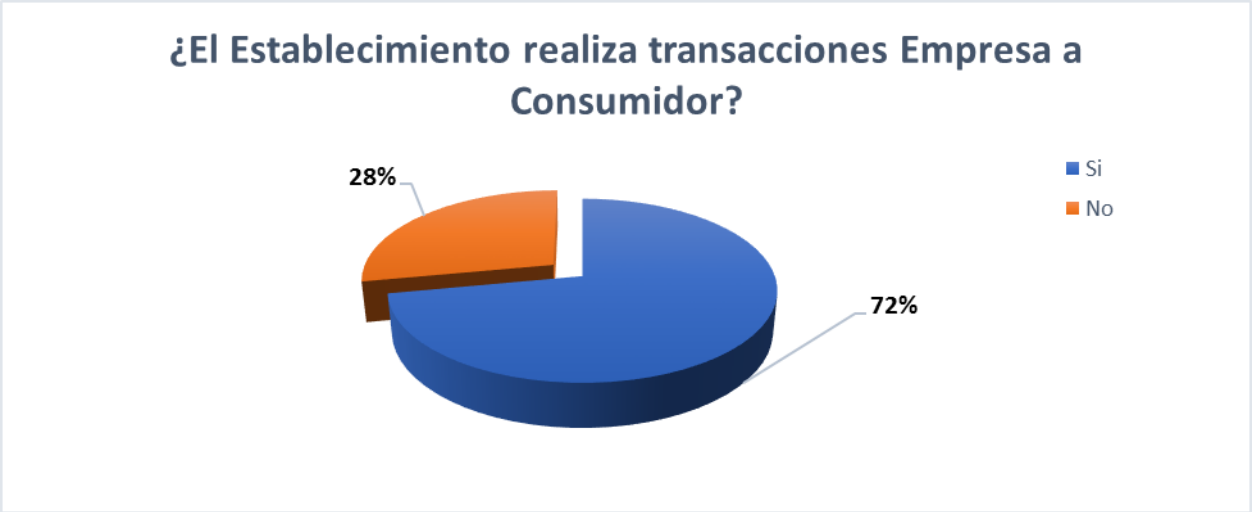
[22]Tipos de comercio electrónico en detalle. *Universidad Americana de Europa* [en línea], 2020. [Consulta: 7 junio 2022]. Disponible en: https://unade.edu.mx/tipos-de-comercio-electronico/.

puede deberse a diversos factores, por ejemplo, que el rubro al que se dedica no lo requiera y poca familiaridad con el concepto.

En contraste con las respuestas negativas tenemos que el 86% del total de los encuestados afirma realizar este tipo de operaciones, cabe destacar que puede existir mayor seguridad en este ámbito debido a las obligaciones y regulaciones formales exigidas al momento de constituir una empresa sin embargo al no existir un marco regulatorio estas siguen estando expuestas a fraudes. En este caso, hay pocos clientes a los que puedes vender y son más exigentes lo cual puede reducir el nivel de riesgo de fraude y ser una mejor opción dentro del sector económico.

2) B2C - Business to Consumer: Las siglas B2C significan del Negocio al Consumidor.

Grafico 6.



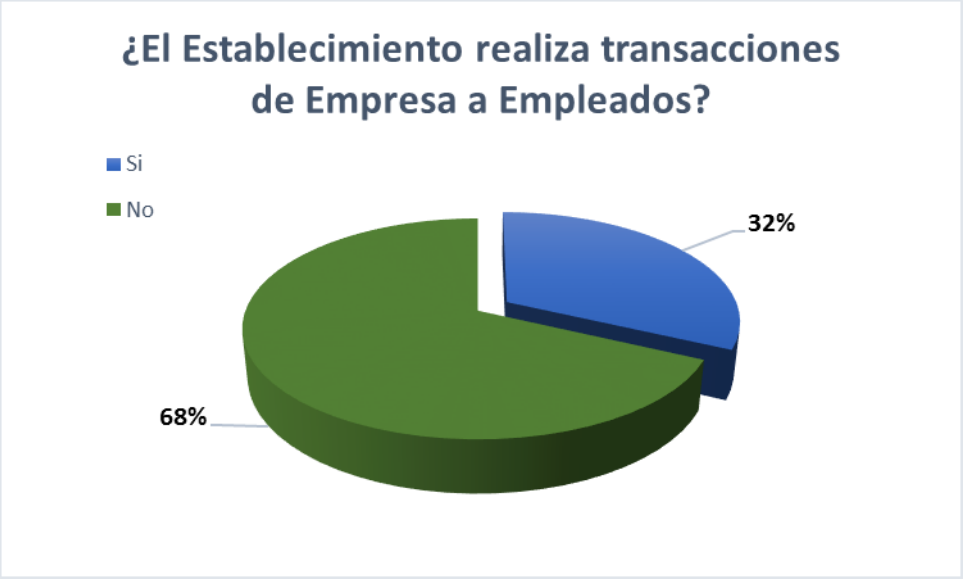
Fuente: Elaboracion Propia. Establecimientos comerciales del centro de la ciudad de León, departamento de León.

Respecto a las transacciones comerciales de empresa a consumidor se observa que el 28% indica no realizar este tipo de operaciones comerciales lo cual de igual manera puede deberse al tipo de rubro de la empresa. En cambio, el 72% de las empresas encuestadas afirma realizar transacciones de empresa a consumidor, es decir que existe una relación directa de compraventa o de prestaciones de servicios, lo cual desafortunadamente puede presentar cierto nivel de riesgo tanto para las empresas como para los mismos consumidores. Se puede mencionar la posible desconfianza del cliente y empresa respecto a la seguridad en los pagos y desconocimiento sobre

la contraparte. En caso de que las empresas no cobren por adelantado esta se arriesga a perder la inversión de la elaboración de este, deben lidiar con la informalidad e irresponsabilidad en el pago y recepción de los pedidos, productos o servicios. A diferencia del *Business to Business*, en esta forma de comercialización las empresas pueden llegar a tener muy poca información sobre la identidad de los consumidores elevando la posibilidad de que esto sea un factor de riesgo para la empresa.

3) B2E - Business to Employee: El comercio "empresa al empleado" es una modalidad relativamente reciente.

Grafico 7.



Fuente: Elaboracion Propia. Establecimientos comerciales del centro de la ciudad de León, departamento de León.

En esta modalidad de transacciones comerciales se observa que apenas un 32% de los encuestados si realiza el *Business to Employees*. Esto puede deberse a las mismas políticas de la empresa que posibilita una forma de transacciones con sus colaboradores de forma interna. Se podría especular que podría ser una forma menos riesgosa de realizar transacciones debido a que hay un mayor control interno por parte de la empresa y se tiene conocimiento pleno de los consumidores aun así es muy poco utilizado.

4) G2C - Goverment to Consumer: del Gobierno al consumidor.

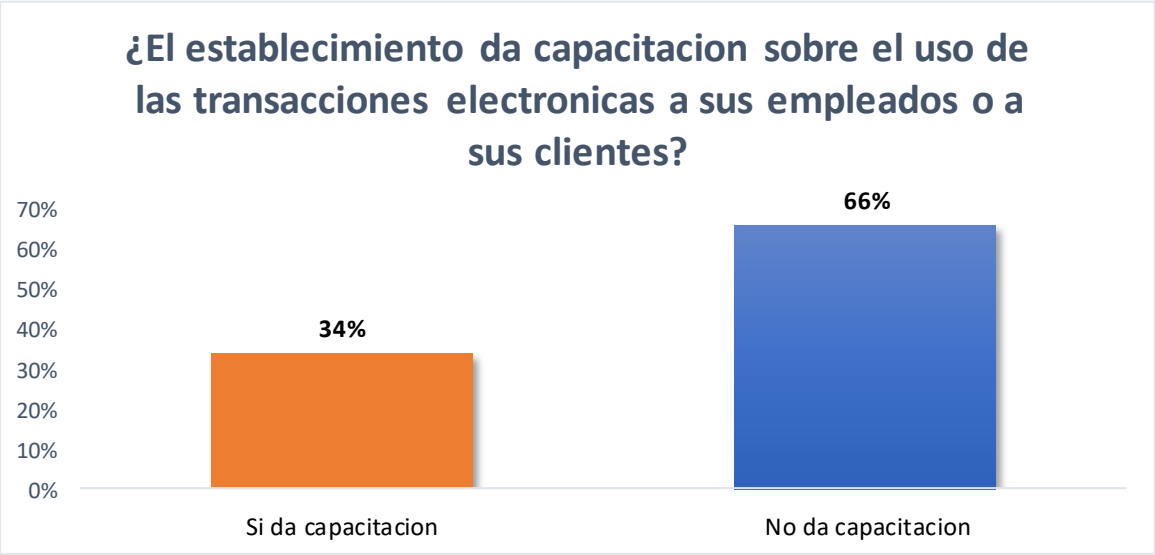
Grafico 8.

Fuente: Elaboracion Propia. Establecimientos comerciales del centro de la ciudad de León, departamento de León.

Respecto a las transacciones comerciales Gobierno a Empresa se observa que el 100% de los establecimientos no realizan este tipo de operaciones comerciales. Lo cual de igual manera puede deberse a la falta de conocimiento sobre las nuevas formas de pago por ejemplo las contribuciones o impuestos que las empresas pueden pagar de manera electrónica hoy en día.

La encuesta también arrojo datos interesantes acerca de la interacción que tienen los establecimientos comerciales con el comercio electrónico, esto abarcando la experiencia que han tenido con el comercio electrónico y el conocimiento y preparación.

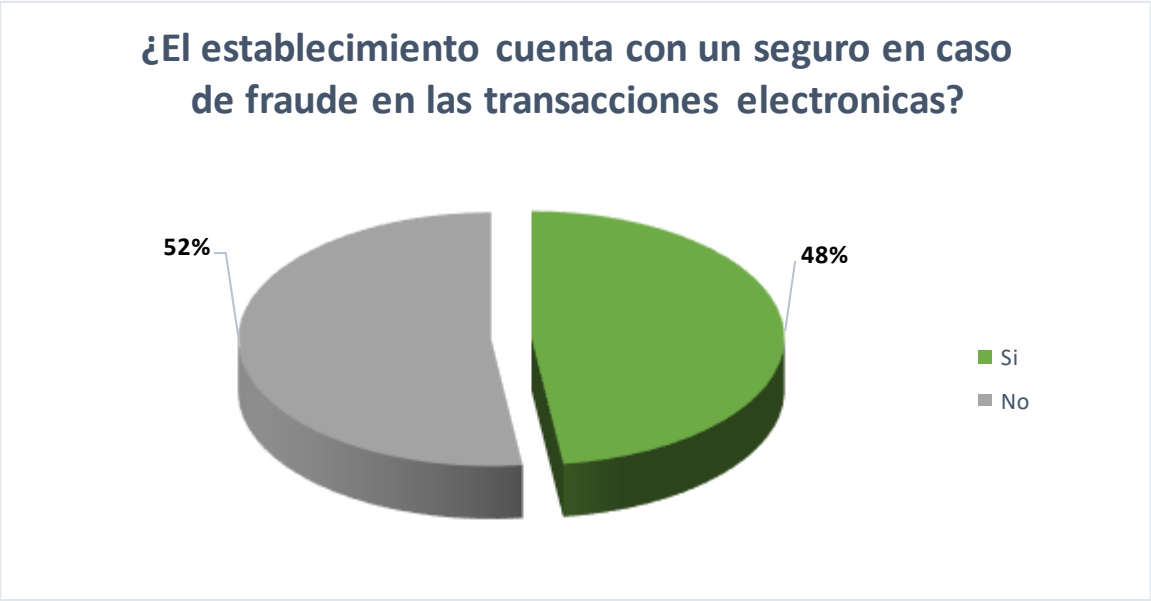
Grafico 4.



Fuente: Elaboracion Propia. Establecimientos comerciales del centro de la ciudad de León, departamento de León.

Se muestra que un 66% de los establecimientos encuestados no brindan capacitaciones sobre el uso de transacciones electronicas a sus empleados o a clientes, solamente un 34% brinda capacitaciones, se podria especular que los establecimientos no cuentan con el debido conocimiento acerca del comercio electronico como para ellos brindar capacitaciones a sus empleados o a sus clientes, esto vulnera las transacciones electronicas ya que no se tienen conocimiento de su funcionamiento.

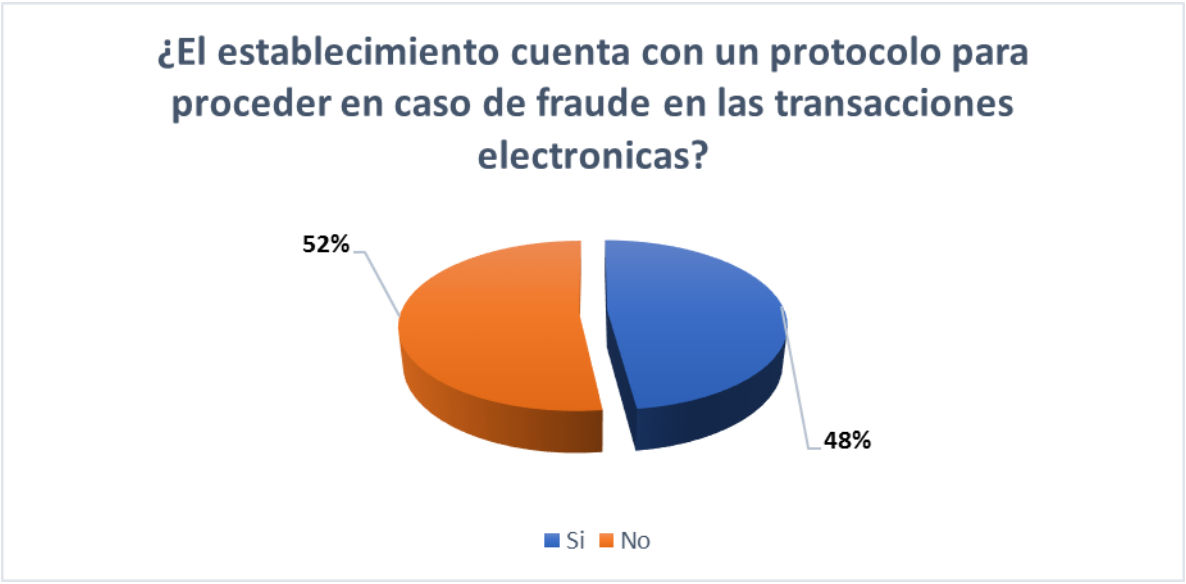
Grafico 5.



Fuente: Elaboracion Propia. Establecimientos comerciales del centro de la ciudad de León, departamento de León.

En base a los seguros en las transacciones electronicas un 48% de los establecimientos encuestados hace uso de los seguros generalmente ofrecidos por los bancos, un 52% establecio no hacer uso de seguros en las transacciones electeonicas que realiza el establecimiento, esto tiende a vulnerar la demanda de este tipo de comercio, creando un tabu en los consumidores que deciden optar por mecanismos mas tradicionales.

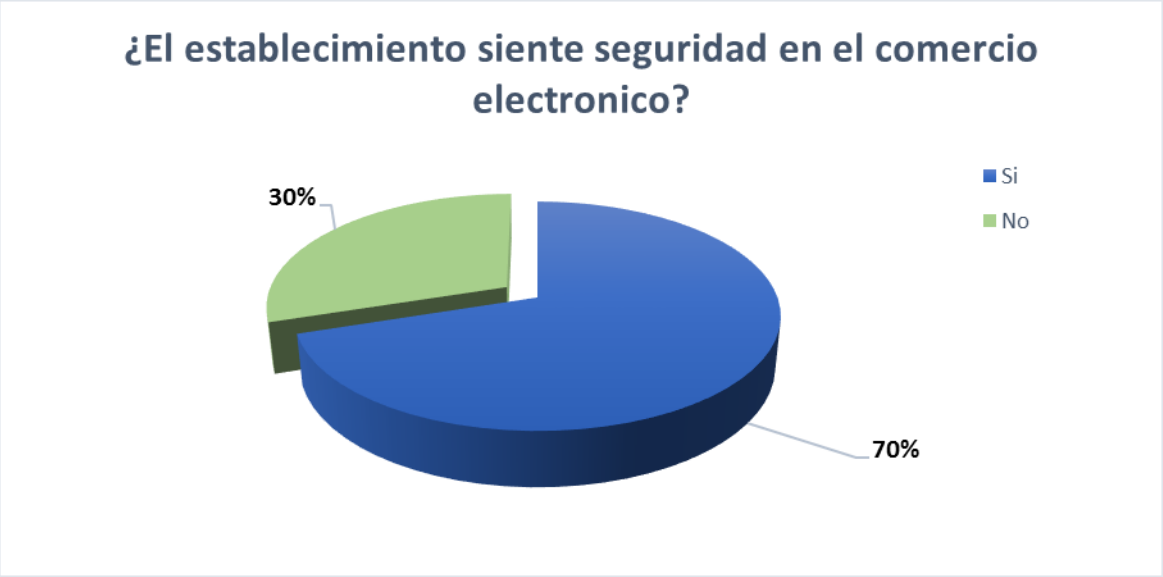
Grafico 6.



Fuente: Elaboracion Propia. Establecimientos comerciales del centro de la ciudad de León, departamento de León.

Un protocolo para proceder en caso de fraude es una de las herramientas mejor posicionadas al momento de que una transaccion electronica sufre fraude, el 52% de los establecimientos encuestados establecio no tener un protocolo de respuesta a una situcion en la que se sufra fraude electronico, solo un 48% de los establecimientos posee un protocolo de respuestas a estas situaciones los cuales generalmente incluyen una dependecia a otras instituciones como el banco.

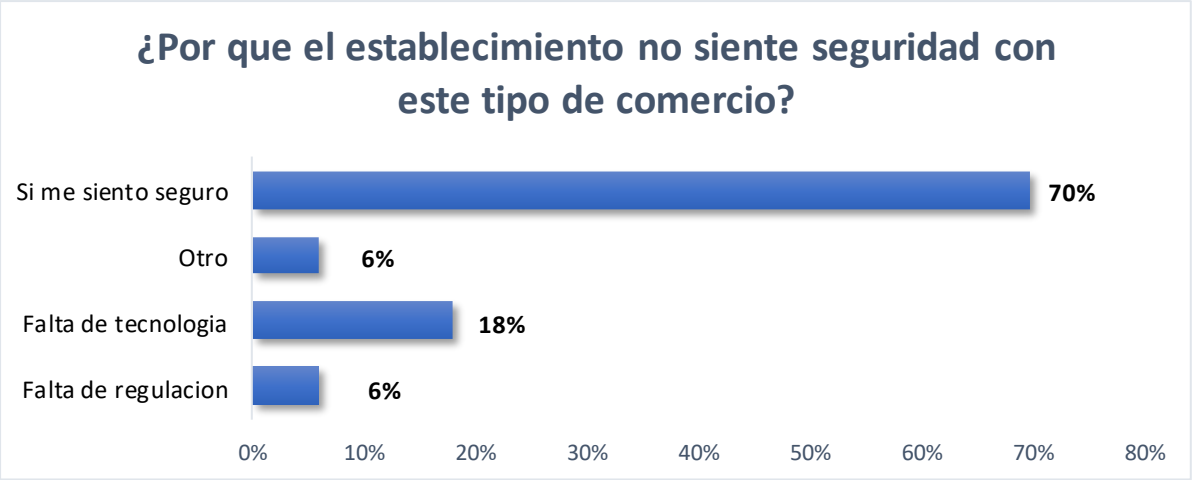
Grafico 13.



Fuente: Elaboracion Propia. Establecimientos comerciales del centro de la ciudad de León, departamento de León.

La seguridad en el comercio electrónico es algo vital para los establecimientos, un 70% de los establecimientos encuestados siente seguridad en el comercio electrónico, contra un 30% que no siente seguridad, es sorprendente tomando en cuenta que muchos de los establecimientos que sienten seguridad no cuentan con seguro, ni con protocolo de respuestas en caso de fraude.

Grafico 14.



Fuente: Elaboracion Propia. Establecimientos comerciales del centro de la ciudad de León, departamento de León.

El 18% de los establecimientos encuestados estableció no sentir seguridad en el comercio electrónico por falta de tecnología, como los medios adecuados para realizar las transacciones electrónicas, otro 6% refleja no sentir seguridad en el comercio electrónico debido a la falta de regulación que existe en nuestro país.

Capítulo II: Marco jurídico regulador de las transacciones electrónicas en Nicaragua

2.1 En la Constitución Política de Nicaragua

Si bien se ha mencionado a lo largo de esta investigación la falta de regulación para el funcionamiento de las transacciones electrónicas de manera fluida y sin riesgos en Nicaragua, si se reconoce la vigencia de un marco normativo a nivel constitucional expresado en el artículo 98, en el cual nos menciona y nos deja claro que una de las funciones principales del Estado en la económica es lograr el desarrollo humano sostenible en el país[23], así como ser un facilitador de la actividad productiva para que las personas realicen su actividad económica, productiva y laboral en un marco de seguridad jurídica plena, por lo mismo, el Estado es y será el responsable de proteger el derecho de las personas consumidoras frente a estas nuevas formas ilícitas de sustracción de liquidez y de información que sufren día a día las personas en Nicaragua.

Aunque, el ejercicio de la actividad económica corresponde principalmente a los particulares como lo menciona el artículo 99 de la constitución política es necesario que el Estado promueva y tutele nuevas formas para garantizar los intereses y las necesidades sociales[24], en este caso darle seguridad jurídica a esas nuevas formas de hacer transacciones de mercancía y dinero a través de internet frente a las nuevas formas de fraude que si bien todavía no están reguladas se conocen y se aplican en Nicaragua.

2.2 Ley Especial de ciberdelitos

Ley especial de ciberdelitos, cuenta con un acápite llamado delitos informativos en los cuales nos hace saber sobre los fraudes informáticos en el que cualquier persona que manipule sistemas, datos o cualquier otra información las cuales pueden ser estadísticas, números, descriptores, que por separado no tienen relevancia para los usuarios del sistema, pero que en conjunto pueden ser interpretados para obtener una información completa y específica para un aprovechamiento en perjuicio ajeno.

[23] Artículo 98. CONSTITUCIÓN POLÍTICA DE LA REPÚBLICA DE NICARAGUA. última Reforma en 2014.
[24] Artículo 99. IDEM.

Por lo mismo, esta ley especial viene a tratar estas nuevas figuras que comenzaron a realizarse antes de que nuestro sistema jurídico contemplara dicho escenario, razón por la cual se han ido formulando poco a poco instrumentos legales para su control que hoy no son suficientes para proteger los intereses (el patrimonio, la confidencialidad de la información, el derecho de propiedad sobre un sistema informático y la seguridad jurídica) de las personas afectadas.

El Hacking o espionaje informático, es una de las principales vías en la cual se accede a información sensible para posteriormente utilizarla en perjuicio del Usuario, estos ataques van dirigidos a través de los TIC (Tecnologías de las información y de la comunicación) que no son más que el conjunto de recursos, herramientas, equipos, programas informáticos, aplicaciones, redes y medios; que permiten la compilación, procesamiento, almacenamiento, transmisión de información como: voz, datos, texto, video e imágenes. Sin embargo, en Nicaragua con la entrada en vigor de la ley 1042, en su artículo 13 nos deja claro que estas conductas antes descritas vienen a proteger además de los intereses de las personas afectadas[25], así también protege la seguridad soberana del Estado de Nicaragua, también las operaciones de las instituciones que en cualquier momento pueden resultar afectadas.

Sin embargo, la legislación todavía no tiene tipificado de manera específica cada una de estas formas de Hacking, de las cuales las más populares y sencillas de manejar son: SPYWARE[26], que es la creación de un software malicioso que infecta el dispositivo electrónico y recopila información sobre el usuario, navegación, aplicaciones y uso habitual de internet, SNIFFER que básicamente es un software que capturan e inspecciona los paquetes de datos que viajan a través de internet, en los cuales va toda la información del dispositivo en el cual se está aplicando dicho software, si bien es cierto que tiene un uso legítimo, los ciberdelincuentes lo han utilizado para supervisar el uso de Internet, incluyendo los correos electrónicos y los mensajes instantáneos y acceder a las credenciales de inicio de sesión, información privilegiada y datos

[25] Artículo 13. LEY Nº. 1042. LEY ESPECIAL DE CIBERDELITOS. aprobada el 27 de octubre de 2020 Publicada en La Gaceta, Diario Oficial Nº. 201 del 30 de octubre de 2020

[26] MALWAREBYTES, 2018. Spyware. *Malwarebytes* [en línea]. [Consulta: 12 febrero 2022]. Disponible en:https://es.malwarebytes.com/spyware

financieros[27]. KEYLOGGER, son programas que se utilizan para registrar y reenviar a su creador todas las pulsaciones que se realizan en el teclado del dispositivo para posteriormente detectar claves y usuario para acceder a información.

Si no, que más bien se encasillan en un solo delito el cual seria "Hurto por medios informáticos" pero es fundamental entender que, si bien tienen el mismo fin, no tienen ni la misma complejidad ni el mismo rango de éxito, por lo tanto, debería ser tipificado de manera separada para así poder identificar y poder resolver con celeridad.

2.3 Ley De Protección De Los Derechos De Las Personas Consumidoras Y Usuarias

La ley 842 ha venido a ser de gran ayuda para darle un marco legal a los derechos de las personas consumidoras para garantizar y promover el consumo responsable, asimismo, darles igualdad y el libre acceso a las disponibilidades que existen en el mercado sobre bienes y servicios de calidad que respondan a sus necesidades humanas básicas.

Por eso, a la creación de dicha ley y el crecimiento de las redes sociales en Nicaragua, se comenzó a explotar el mercado electrónico informal mediante el uso de internet, siendo este uno de los más vulnerables en cuanto a fraudes se tratase, puesto que al realizar estas transacciones en muchos casos las personas consumidoras han sido víctimas de cualquier tipo de acciones sin ninguna garantía como pueden ser falsa información y mal estado del producto que se está ofreciendo, así como cobrar un precio de venta superior al publicado, adulteración de los productos e incluso la falsificación de un producto.

Para esto, la ley 842 ya hace mención a las transacciones electrónicas en su artículo 77 en el cual dice que: *"Las transacciones por medios electrónicos son aquellas efectuadas entre personas proveedoras y las consumidoras y usuarias a través del uso de medios electrónicos, digitales o de cualquier otra tecnología…"*, así mismo, en los artículos siguientes nos habla de cómo los proveedores deben dar la información verídica sobre dichos productos, bienes o

[27]BELCIC, I., 2020. *¿Qué es un Sniffer y cómo puede protegerse?* [en línea]. [Consulta: 15 d febrero 2022]. Disponible en: https://www.avast.com/es-es/c-sniffer.

servicios porque dicha ley prohíbe las prácticas comerciales engañosas respecto a las características de dicho producto que pueden inducir al fraude o confusión para las personas consumidoras o usuarias.

Sin embargo, en la parte del procedimiento y las sanciones para aquellas personas que incurran en fraudes sobre productos o servicios, la ley 842 es clara al decir que el órgano rector de las protección de los derechos de las personas consumidoras es a través de la Dirección General de Protección de los Derecho de las Personas Consumidoras y Usuarias (DIPRODEC), así como en los casos de materia de servicios financieros corresponderá a la Super Intendencia de Bancos y Otras Instituciones Financieras (SIBOIF) y a la Comisión Nacional de Microfinanzas (CONAMI).

En cuanto al procedimiento, en el artículo 99 se puede ver como la ley nos habla de un procedimiento meramente administrativo[28] y de cómo las personas afectas pueden realizar su reclamo ante la persona proveedora y laDirección General de Protección de los Derechos de las Personas Consumidoras o Usuarias(DIPRODEC), igualmente las sanciones que se pueden aplicar en estos casos son administrativas, por lo tanto, se puede decir que si bien la ley 842regula muchos aspectos de las transacciones electrónicas que pueden ser muy importante al momento de que se pueda presentar cualquier tipo de fraude no tiene la fuerza coercitiva que estos delitos ameritan.

Al mismo tiempo, el procedimiento administrativo termina siendo un poco tedioso para la persona consumidora afectada puesto que el trámite puede llevar su tiempo si es que es admitida dicha denuncia y resuelta, en definitiva, muchas personas afectadas toman la decisión de no llevar el procedimiento y simplemente dejar pasar el caso, en este aspecto resulta algo negativo puesto que la ley tiene como objetivo velar y garantizar los derechos de las personas consumidores.

2.4 Ley General de Telecomunicaciones y Servicios Postales

[28]Artículo 99. LEY Nº. 842. *LEY DE PROTECCIÓN DE LOS DERECHOS DE LAS PERSONAS CONSUMIDORAS Y USUARIAS*. Aprobada el 13 de junio de 2013. Publicada en La Gaceta, Diario Oficial Nº. 129 del 11 de julio de 2013

La Ley de Telecomunicaciones tiene por objeto establecer el marco legal de manera general de las telecomunicaciones y servicios postales que se tiene en nuestro país, con el fin de garantizar el derecho humano de las personas a la comunicación y a la realización de las actividades económicas.

Según estimaciones de la Unión Internacional de Telecomunicaciones, sólo de 20 a 25% de la población mundial goza de los beneficios de las telecomunicaciones, dada la digitalización en todos los campos del saber y de la vida diaria.(Nota alpie) La incorporación de la digitalización y la Internet a las telecomunicaciones crearon la disciplina conocida como Telemática en donde el concepto de "Redes y Movilidad" juegan un papel preponderante y están afectando los mercados, aplicaciones tecnológicas y los aspectos reguladores y normativos actuales.

2.5 Ley General De Bancos Y Otras Instituciones Financieras y Norma sobre Gestión de Riesgo Tecnológico SIBOIF

Tiene por objeto regular las actividades de intermediación financiera donde se incluye los recursos, operaciones, transacciones y de prestación de otros servicios financieros esto con el fin de dar estabilidad al sistema financiero y bancario de Nicaragua proporcionando la oportunidad de poder otorgar créditos o financiamiento para las inversiones a los bancos y otras entidades financieras como entidades de ahorro, financieras, operadores de tarjeta de crédito y otras instituciones financieras.

Así pues, se crea la Super Intendencia de Bancos y otras Instituciones Financieras (SIBOIF) quien es la encargada de velar por los intereses de los depositantes quienes confían sus fondos a las instituciones financieras, legalmente autorizadas para recibirlos y preservar la seguridad y confianza del público en dichas instituciones, promoviendo una adecuada supervisión que procure su solvencia y liquidez en la intermediación de los recursos a ellos confiados.

Igualmente, la SIBOIF tiene a su cargo autorizar, supervisar, vigilar y fiscalizar el funcionamiento de todos los bancos, sucursales y agencias bancarias que operen en Nicaragua, así como instituciones financieras no bancarias, que operen con recursos del público. Al mismo tiempo, la superintendencia tiene que promover que las instituciones bancarias y financieras

cuenten con un sistema de control de riesgos que les permita identificar, limitar y controlar dichos riesgos con el fin de eliminar el posible impacto negativo que pueden enfrentar en el desarrollo de sus actividades, así como los riesgos operativos, los cuales pueden generarse por deficiencias o fallas en los procesos internos, también en la Tecnología de información y comunicación, los antes mencionados (TIC), en las personas y por eventos externos es decir algún agente que busque realizar cualquier tipo de fraude a estas instituciones. Para esto, El consejo Directivo de la SIBOIF da la Norma sobre Gestión de Riesgo Tecnológico con fecha del 19 de septiembre de 2007, en el cual en su artículo 28 donde nos habla de la Seguridad de Personal[29], en el que las instituciones deberán definir los procedimientos para reducir los riesgos asociados a robos, fraudes o mal uso de activos, vinculados al riesgo de TIC.

Es necesario poder definir adecuados roles y responsabilidades sobre la información y su procedimiento, igualmente definir procedimientos de contratación de personal, especialmente para el manejo de procesos críticos de Tecnología de información y comunicación, también el poder establecer la firma de acuerdos de confidencialidad por los empleados y personal externo al que se le brinde acceso al sistema de información.

2.6 Comparación entre leyes internacionales y la legislación nicaragüense

2.6.1 Ley Gramm-Leach-Bliley

La Ley Gramm-Leach-Bliley (GLB Act o GLBA), también conocida como Ley de Modernización de Servicios Financieros de 1999, es una ley federal promulgada en los Estados Unidos para controlar la forma en que las instituciones financieras tratan la información privada de los individuos[30]. Esta ley vino a reformar la industria de servicios financieros, permitiendo que los bancos comerciales y de inversión, las empresas de valores y las compañías de seguros se consolidaran y abordaban las preocupaciones sobre la protección de la privacidad frente a la gran cantidad de fraudes que sufrían los consumidores.

[29] Artículo 28. *NORMA SOBRE GESTIÓN DE RIESGO TECNOLÓGICO.* Resolución Nº CD-SIBOIF-500-1-SEP19-2007 De fecha 19 de septiembre de 2007.
[30] Gramm-Leach-Bliley Act (GLBA). 1999.

Si se realizauna comparación sobre esta ley estadounidense en la legislación Nicaragüense, la ley especial de ciberdelitos tiene por objeto la prevención, investigación, persecución y sanción de los delitos cometidos por medio de las Tecnologías de la Información y la Comunicación, en perjuicio de personas naturales o jurídicas, donde en el capítulo II tutela y sanciona cualquier delito mediante cualquier dispositivo de la TIC relacionado con la información sensible de las personas en los bancos, instituciones de finanzas y grupos financieros, así mismo, con el fraude electrónico la ley especial de ciberdelitos lo tutela, igualmente la ley Gramm-Leach-Bliley en su primera sección nos habla de la Regla de Privacidad Financiera, que es la que regula la recopilación y divulgación de información financiera privada de las personas frente a los diferentes delitos de espionaje y fraudes electrónicos que pueden sufrir siendo estos Keylogger y Sniffer, los tipos de fraudes que sufren los sistemas de intercambio de información mediante la Tecnología de la información y la comunicación.

2.6.2 Ley Federal De Protección Al Consumidor México

La ley federal de protección al consumidor[31] (Estados Unidos Mexicanos) publicada en el Diario Oficial de la Federación el 24 de diciembre de 1992 que tiene por objeto promover y proteger los derechos y cultura del consumidor y procurar la equidad, certeza y seguridad jurídica en las relaciones entre proveedores y consumidores. En lo referente a Comercio Electrónico en su capítulo VIII establecido como derechos de los consumidores en las transacciones efectuadas a través del uso de medios electrónicos, ópticos o de cualquier otra tecnología, en las que en su art. 76 establece la responsabilidad del proveedor en la práctica comercial, la confidencialidad de la transición, así como la protección de los datos del consumidor, la autenticación del servicio o local físico, los términos y condiciones del servicio ofrecido. En comparación con la Ley N°. 842 ley de protección de los derechos de las personas consumidoras y usuarias, aprobada 13 de junio de 2013 Publicada en La Gaceta, Diario Oficial

[31]Congreso De, D. And Unión, L. [Sin Fecha]. LEY FEDERAL DE PROTECCIÓN AL CONSUMIDOR. Capítulo I Disposiciones Generales. [En Línea]. S.L.: Disponible En:https://www.profeco.gob.mx/juridico/pdf/l_lfpc_ultimo_camdip.pdf

N°. 129 del 11 de julio de 2013. Que tiene el mismo objeto de protección no presenta una capitulación especial acerca de la protección de los derechos de los consumidores en las transacciones electrónicas solamente presenta el art. 65 referente a las transacciones electrónicas de los servicios financieros hablando del reconocimiento de la legalidad de la misma, el art 77 y 78 establece la responsabilidad de la parte proveedora la información verídica y actualizada sobre su domicilio físico, el art. 79 establece la seguridad de las transacciones electrónicas y sistemas de seguridad por parte de la parte proveedora. En conclusión, ambas legislaciones contemplan el tipo de comercio electrónico y ambas establecen de manera somera las obligaciones del proveedor.

2.7 Derecho Informático

La pandemia por *Covid*-19 ha forzado una migración de muchos de los procesos a los medios digitales, por esta razón, el derecho informático. En la conceptualización de derecho informático refiere Olivera[32]que fue utilizado e introducido en el vocabulario jurídico por el Profesor Dr. Wilhelm Steinmüller de la Universidad de *Regensburg*, ciudad situada al este del Estado de Baviera, Alemania, su origen deviene de la voz *Rechtinformatik*.- En segundo término, se puede conceptualizar esta incipiente rama jurídica, siguiendo el método aplicado por la doctrina cuando define una disciplina del derecho, "como un conjunto ordenado y sistemático de principios y normas, que regulan las conducta, comportamientos, relaciones y los efectos jurídicos consecuencia de la actividad informática, usos, aplicaciones e implicancias legales. ha cobrado gran importancia al proporcionar legalidad y certeza a estos procesos.

El Derecho Informático igual se concibe como la rama del Derecho que regula los efectos jurídicos derivados de la informática y de las Tecnologías de Información y Comunicación (TIC). Se especializa, además, en el estudio de las transformaciones del Derecho como consecuencia del uso generalizado de las actividades tecnológicas. La informática se caracteriza por ser un ámbito muy cambiante, por este motivo, esta ciencia jurídica analiza las

[32] OLIVERA, Noemí "Reflexiones en Torno al sistema Jurídico de la Sociedad de la Información. LL UNLP 2008 – 38, 597

modificaciones de la informática y/o las *TIC* respecto a la sociedad, con la finalidad de crear principios y normativas que logren regularla adecuadamente[33].

Los beneficios que aporta el derecho informático han de entenderse en base a los siguientes principios:

1- Principio de equivalencia funcional.

Refiere que, teniendo un soporte legal robusto, un documento emitido, firmado, y consensuado por las partes implicadas de manera escrita, tiene la misma validez qué el mismo documento en soporte informático. Es decir que dicho documento digital es igual de válido que su homólogo en físico.

Esto además da garantías a las partes de que un documento no va a sufrir daños o a desaparecer, como sí ocurre con los documentos físicos. Una vez en digital, puede ser almacenado en discos duros, nube, memorias USB, etc. Un documento puede verse afectado no solo por accidentes o descuido del portador. En muchas ocasiones, el propio material del documento puede hacerlo propenso a daños. Ciertos tipos de papel y tinta tienden a dañarse con las altas temperaturas, por ejemplo. Gracias a las nuevas herramientas para la emisión y firma de documentos de forma electrónica, se facilita en inmensa medida el proceso de firma de contratos[34].

2.- Principio de neutralidad electrónica

---

[33] MONROY, P., 2021. ¿Qué es el Derecho informático? *Soycest.mx* [en línea]. [Consulta: 21 julio 2022]. Disponible en: https://www.soycest.mx/blog/index.php/derecho-informatico.

[34] CERTIMATCH CONFIANZA DIGITAL, 2022. ¿Qué es el derecho informático y porqué es importante conocerlo? - CertiMatch. *CertiMatch* [en línea]. [Consulta: 21 julio 2022]. Disponible en: https://certimatch.com.mx/que-es-el-derecho-informatico-y-porque-es-importante-conocerlo/.

Las leyes sobre la neutralidad electrónica de los documentos son claras. No puede haber favorecimiento en el marco legal sobre el uso de una herramienta sobre otra. Siempre y cuando las herramientas en cuestión cuenten con la misma validez jurídica, las leyes serán neutrales en cuanto a la herramienta o plataforma elegida por las partes.

La constante aparición de nuevas tecnologías también obliga a las leyes a ser multi formato, multi estándar, multiprotocolo y multi algoritmo.

3.- Transparencia

La gran preocupación de muchas personas al pensar en documentos electrónicos es lo fácil, en principio, que parece falsificar una firma o editar un documento. Sin embargo, lo cierto es que las firmas electrónicas son extremadamente seguras.

Por ejemplo, las normativas mexicanas dentro del servicio de la Constancia de la Conservación permiten garantizar la identidad de los firmantes y la veracidad del documento con el uso de los certificados electrónicos establecidos en la NOM-151. También es posible por medio de los sellos de tiempo verificar el momento exacto en el que se generó el documento o la firma.

Otro punto por tomar en cuenta en el derecho informático es que son y serán leyes en constante evolución. Esto quiere decir que las leyes sobre el derecho informático no son definitivas y estarán sujetas a cambios con el paso del tiempo. Aparecerán nuevas tecnologías que aporten a la práctica del derecho, por lo que surgirán junto a ellas nuevas normas y regulaciones.

También se espera que las normas existentes desaparezcan o sean modificadas en base a qué herramientas se usen en el futuro y cómo se pongan en práctica. Por ende, hay que estar actualizados sobre los avances de la tecnología en el plano del derecho en los próximos años.

La innovación consiste en la modificación de los elementos ya existentes con el fin de mejorarlos, y esto aplica perfectamente al derecho informático. Estas normativas están apenas en sus primeras etapas en muchos países y se espera que, con su uso y el paso del tiempo, se descubran nuevas formas de aplicar los reglamentos.

Características del derecho informático

Es un derecho moderno, en comparación con otras ramas tradicionales del Derecho, que tiene sus orígenes en los problemas generados por la Implementación de la computadora en la sociedad. Se recordará que el impulso y posterior desarrollo de las computadoras data de los años 50 del siglo XX[35].

Es un derecho íntimamente influenciado por las tecnologías en general, debido a que éstas han permitido un desarrollo sostenido de la computadora y su entorno, por ejemplo, en la actualidad se tienen una serie de problemas jurídicos generados por el uso de Internet en las diversas actividades de las personas.

Es un derecho que se encuentra ligado al proceso de globalización, por lo que el jurista se encuentra obligado a resolver el problema del juez competente, el mismo que debe conocer y dar solución a determinado caso concreto, debiendo, asimismo, analizar todo aquello que esté relacionado con la ley aplicable a cada situación en particular.

Es un derecho que necesariamente debe ser legislado en leyes especiales, debido a que su objeto de estudio, así como sus formas de regulación son muy dinámicas.

Es un derecho autónomo, con instituciones propias que se encarga de brindar soluciones legales a los problemas planteados por el avance científico en el ámbito de su competencia. Es importante indicar, que conforme transcurre el tiempo surgen nuevas dificultades legales no previstas por el jurista, el legislador o el juez, pero que el Derecho informático permite solucionar, hecho que refuerza y sustenta la característica en mención.

Aplicación del derecho informático

Puesto que podemos decir que el Derecho Informático y las nuevas tecnologías van de la mano, el ámbito de aplicación de esta rama del Derecho es muy amplia; más allá de los crímenes cometidos a través de la informática, también se aplica en el derecho a la privacidad, el honor y

[35] Derecho Informático | Carlos Felipe Law Firm. *Fc-abogados.com* [en línea], 2022. [Consulta: 21 julio 2022]. Disponible en: https://fc-abogados.com/es/el-derecho-informatico-y-su-alcalce-regulador/.

la propia imagen, la protección de datos, las redes sociales, el comercio electrónico, la seguridad informática, la publicidad online, la defensa de los consumidores, la regulación del teletrabajo, los trámites telemáticos o los certificados y firmas digitales.

Derecho Informático dentro de las demás ramas del derecho

El derecho informático cuenta, al igual que las demás ramas de derecho, con sentencias de tribunales y razonamientos de teóricos del derecho. Las fuentes del derecho informático afectan a las ramas tradicionales del derecho:

En el Derecho Público

- Derecho de acceso universal a Internet
- Flujo internacional de datos informatizados
- Protección de datos
- Libertad informática (defensa frente a eventuales agresiones)
- Delitos informáticos (tienden a crear un ámbito propio del Derecho Penal)

En derecho privado

- Contratos informáticos (hardware, software)
- Protección jurídica de los programas de ordenador
- Lo que aún se discute en la actualidad es si este derecho es una nueva disciplina o es una serie de normas dispersas que engloba a varias disciplinas.

Importancia del derecho informático

El Derecho informático cumple un rol importante en la prevención de situaciones no deseadas para los usuarios de las Nuevas Tecnologías de la Información y cuando se presentan determinadas circunstancias que los afecten, facilita la incorporación de nuevas instituciones jurídicas que permitan crear confianza a las personas e instituciones que realizan tales operaciones, permitiendo de esta forma la solución de aquellos problemas generados por el uso de los medios electrónicos en la sociedad.

Diferencia entre informática jurídica y derecho informático

La informática jurídica es la ciencia que estudia el empleo de los recursos informáticos para mejorar los procesos, análisis, investigación y gestión en el ámbito jurídica. Es decir, es el empleo de software y hardware como instrumentos del derecho, para agilizar los procesos legales. No se trata de una rama del Derecho, sino de las herramientas que se pueden utilizar dentro de este campo, como puede ser, por ejemplo, Lexnet, el sistema de gestión de notificaciones telemáticas dese los juzgados a los abogados.

Mientras que el Derecho Informático, como ya hemos dicho, es ese conjunto de principios y normas que regulan los efectos jurídicos de la relación entre el Derecho y la informática y es propiamente una rama especializada del Derecho.

Dentro del Derecho informático se encuentran fraudes como:

- Fraude Mediante Uso De Computadora;
- Accesos No Autorizados;
- Destrucción De Programas O Datos;
- Reproducción No Autorizada De Programas Informáticos;
- Uso No Autorizado De Programas Y Datos.

Capítulo III: Tipos de fraude que se presentan en las transacciones electrónicas en los establecimientos comerciales del municipio de León, Nicaragua

En nuestra sociedad actual, las tecnología de la información y comunicación (TIC) han encaminado nuestro día a día como personas a una realidad ligada estrictamente a la tecnología, a tal punto que en Internet se encuentran millones de personas que parecieran estar interconectadas, esto debido al fácil acceso y a la cantidad de información que los usuarios insertamos en ella, de tal manera que ahora muchos sistemas e instituciones en ámbitos como seguridad, comercio, comunicación, bancarios y transporte, se pueden realizar mediante la red[36]. Sin embargo, no todo ha sido de manera positiva, puesto que han surgido nuevos y cada vez más frecuentes fraudes que han afectado las transacciones electrónicas que realizan muchas personas a diario en nuestro país.

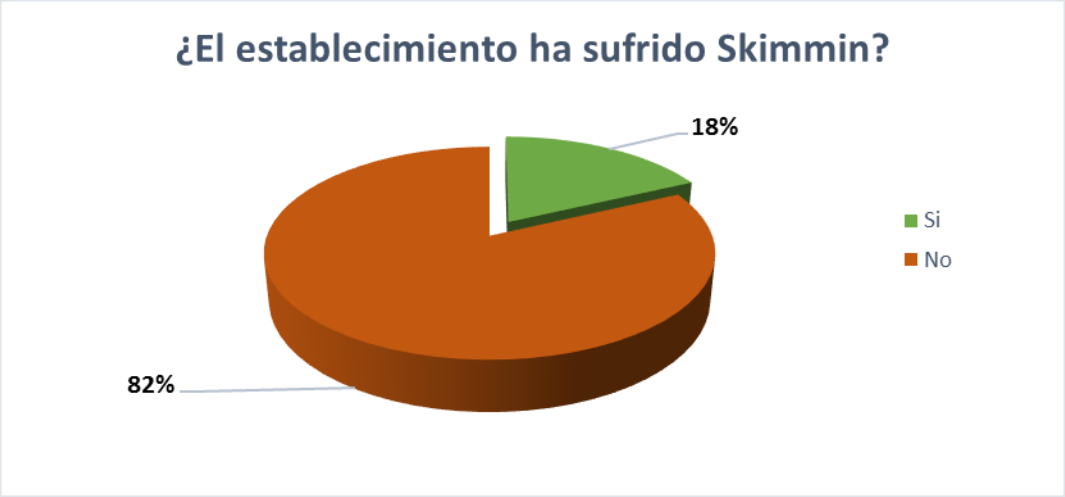
Si bien, el fraude informático no es el único ciberdelito que se ha detectado en Nicaragua, si es el más sencillo de identificar, esto por el impacto económico y por la frecuencia con el que se ejecutan, el cual se ha visto potenciado por el rápido crecimiento del comercio electrónico, uno de estos factores fue la pandemia de COVID-19 que aumentó el interés y la necesidad de las personas por las compras y pagos online, si bien, esto contribuyo a incrementar las ventas en los E-commerce, creo más oportunidades para la evolución de los diferentes tipos de fraudes.

3.1 Tipos de Fraudes en Nicaragua

1) **Fraudes con tarjeta de crédito o Skimming**: Esta modalidad es muy común en cajeros automáticos y establecimientos comerciales, puesto que es la manera más sencilla de sustraer dinero de las tarjetas ya sea de debido y/o crédito, debido a que la banda magnética que tienen las tarjetas en muchos casos no es segura y el PIN de cuatro dígitos es un código bastante sencillo de descifrar por los informáticos, el objetivo de los delincuentes es permitirse hacer avances y apropiarse del dinero que están en las cuentas bancarias del usuario afectado.

[36] SÁNCHEZ MEDERO, Gemma. *"Delitos en internet: clases de fraudes y estafas y las medidas para prevenirlos*". Madrid. 2012. P. 67-68.

Grafico 16.



Fuente: Elaboracion Propia. Establecimientos comerciales del centro de la ciudad de León, departamento de León.

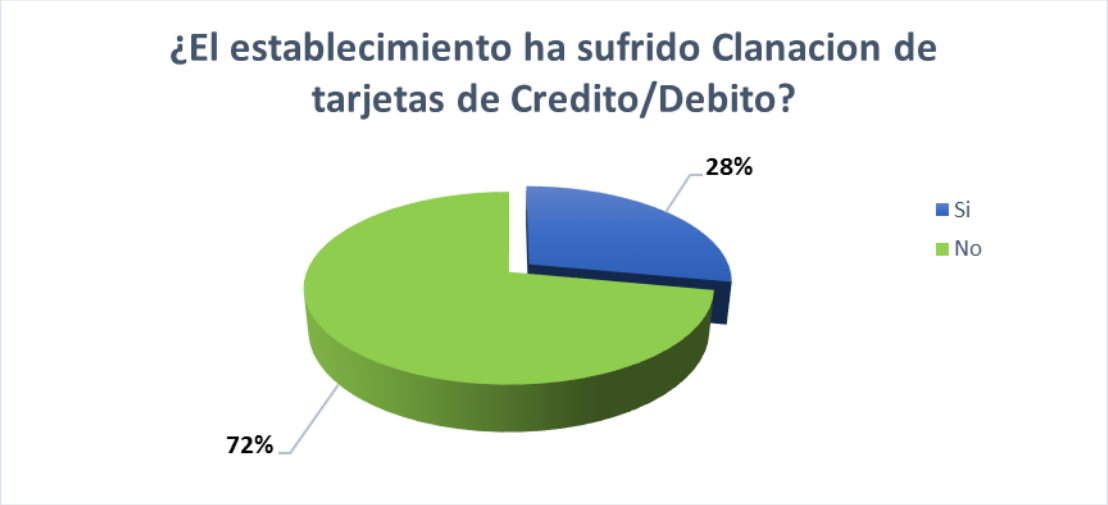
Si bien todavía en Nicaragua el Skimmin no se ha vuelto una de las tácticas fraudulentas más utilizadas por los ciberdelincuentes puesto que el 82% de los establecimientos encuestados no han sufrido de este tipo de fraude, si conocen la existencia de esta forma de sustracción de Dinero y se han ideado diferentes soluciones para prevenirlo, la más común es el correcto uso del POS[37] (Point of Sale) es el aparato por el cual se pasan las tarjetas de Crédito o debido en los establecimientos para el pago por el producto o servicio, los POS normalmente son dados por las entidades bancarias y están registrados, otra forma de prevenir el Skimmin es cambiar las tarjetas de crédito después de 3 años de uso, esto debido al desgaste y desactualización de la banda magnética con la que vienen integrada.

2) **Clonación de tarjetas**: Mediante el uso de dispositivos especializados como falsos teclados, cámaras espías, entre otros, los delincuentes logran obtener información que les va permitir hacer una copia de la tarjeta original y a partir de la información obtenida previamente (claves personales), podrán hacer compras y utilizar el dinero del cuentahabiente para lo que ellos

[37] MARIN, RODOLFO. *¿Qué son las terminales POS y cómo ayudan a los comercios? BBVA NOTICIAS* [en línea]. 2020. [Consulta: 5 julio 2022]. Disponible en: https://www.bbva.com/es/ar/que-son-las-terminales-pos-y-los-comercios/.

deseen. El portal web BBC[38] indica que "para este tipo de robo, el dispositivo más utilizado es un 'Skimmer', un aditamento que se inserta en la ranura para la tarjeta en el cajero, el cual tiene una cámara para captar en video que cuando se teclea la clave, la graba instantáneamente y que, además, al deslizar la tarjeta al interior, se captura la información de la banda magnética."

Grafico 17.



Fuente: Elaboracion Propia. Establecimientos comerciales del centro de la ciudad de León, departamento de León.

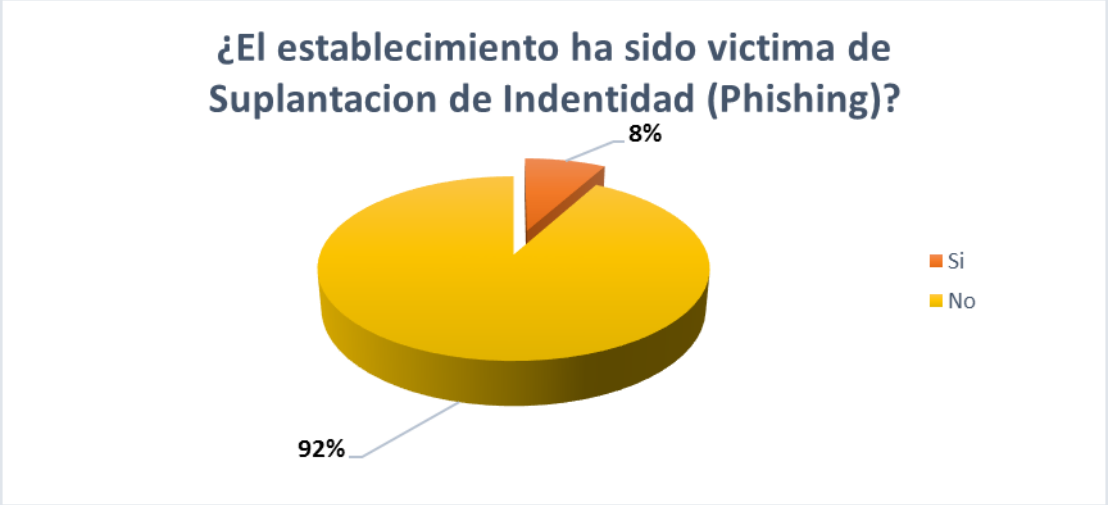
En cuanto a los establecimientos encuestados, el 72% no han sufrido de clonaciones de tarjetas de Crédito/Debito, esto porque este tipo de fraude se realiza a través del uso del aparato llamado Skimmer, ya antes mencionado. Normalmente este dispositivo electrónico es colocado en los cajeros automáticos, sin embargo, el 28% de los establecimientos experimentaron casos en los cuales los han colocados en sus comercios y almacenes en general.

Por otra parte, vemos como cada una de estas figuras van surgiendo a partir de otra, es decir, tanto la clonación de tarjetas de crédito/Debito como el Skimmin buscan afectar la banda magnética de las tarjetas para poder hacer transacciones con los datos obtenidos pero lo que diferencia estos fraudes entre sí es la modalidad de cómo operan.

[38] ORGAZ, Cristina J. *"Prevenir que te clonen la tarjeta bancaria y te roben tus datos".* 29 de mayo del 2019. [Consulta: 5 julio 2022]. Disponible en: https://www.bbc.com/mundo/noticias-48433105

3) **Phishing o suplantación de identidad**: Es de las técnicas fraudulentas más usada para el robo de información personal, credenciales de acceso a servicios online o información bancaria. Su funcionamiento se basa en envío de emails u otro tipo de mensajes suplantando la identidad de algún servicio o empresa conocido para que la víctima acceda a una página fraudulenta que simula ser la legítima, sin siquiera usar su tarjeta. La finalidad es que el usuario introduzca todo tipo de información para queel ciberdelincuente pueda contar con ella.

Grafico 21.



Fuente: Elaboracion Propia. Establecimientos comerciales del centro de la ciudad de León, departamento de León.

El Phishing es la forma más popular a nivel mundial de ciberdelincuencia debido a su eficacia, ya que ha resultado la forma más fácil y rápida para poder engañar a los usuarios mediante correos electrónicos, mensajes de textos, mensajes directos en las redes sociales e incluso en las diferentes plataformas de video juegos[39]. No obstante, el 92% de los establecimientos no han sufrido de Phishing, esto debido que han aprendido formas de reconocer correos o mensajes donde se ve que se trata de este tipo de fraude.

Los establecimientos y los usuarios han logrado identificar los factores comunes que tienen normalmente la suplantación de identidad; primeramente, es la urgencia de la acción, es decir que

[39] MICROSOFT. What Is Phishing, 2022. *Protéjase del phishing*. [en línea]. [Consulta: 5 julio 2022]. Disponible en: https://support.microsoft.com/es-es/windows/-phishing-ataque.

aquellos correos o mensajes que afirman que se debe hacer clic, abrir o llamar a un archivo adjunto de inmediato es porque afirman tener actuar para evitar una sanción de la institución bancaria u otra empresa. Dando a los usuarios un sentido de urgencia, lo que hace que no la piensen demasiado y entren al archivo adjunto y sean una víctima más.

Otro de los factores comunes que tienen los correos de suplantación de identidad es la poca frecuencia además de genéricos y la mala gramática con la cual se reciben, puesto que estos mensajes se mandan de direcciones de correos electrónicos fuera de los oficiales de las instituciones o empresas y con errores ortográficos y gramaticales muy obvios, es seguro que se trate de Phishing.

4) **Smishing**: Esta modalidad de delito utiliza los teléfonos móviles de los usuarios financieros, los delincuentes pretenden suplantar la identidad, a menudo de personal bancario o establecimientos comerciales, -gerentes o representantes de ventas con el fin de que las personas accedan mediante mensaje de texto o llamada a un link que le proporcionara al atacante información necesaria para hackear el teléfono de la víctima.

Grafico 18.

Fuente: Elaboracion Propia. Establecimientos comerciales del centro de la ciudad de León, departamento de León.

En general, el Smishing es de los métodos fraudulentos que más fácil llegan a los usuarios por la sencilla razón que este no requiere siempre de conexión a internet para poder

obtener información sensible puesto que involucra mensajes de textos como medio[40]. Como resultado el 26% de los establecimientos si lo han sufrido porque las personas tienen a confiar más en los mensajes de textos o SMS que en los mismos correos electrónicos porque la mayoría están conscientes del riesgo para la seguridad que conlleva hacer clic en vínculos incluidos en los correos electrónicos, pero no puede decirse lo mismo cuando se trata de mensaje de textos.

Dado que, el Smishing usa elementos de ingeniería social para obtener todo tipo de información desde contraseñas en línea, información de las tarjetas o cuentas bancarias hasta el número del seguro social, sin embargo, alrededor del 74% de las personas y establecimientos no han sufrido de Smishing porque han comenzado a ser muy cuidadosos en todos los ámbitos de sus teléfonos y más cuando se trata de mensajes de textos tan específicos como el caso de decir que si no se entra en dicho vinculo se comenzara a cobrar el uso del servicio de forma diaria o si se ven resúmenes de sus tarjetas de débito o crédito con falsa información de estados de cuenta para entrar en dichos vínculos.

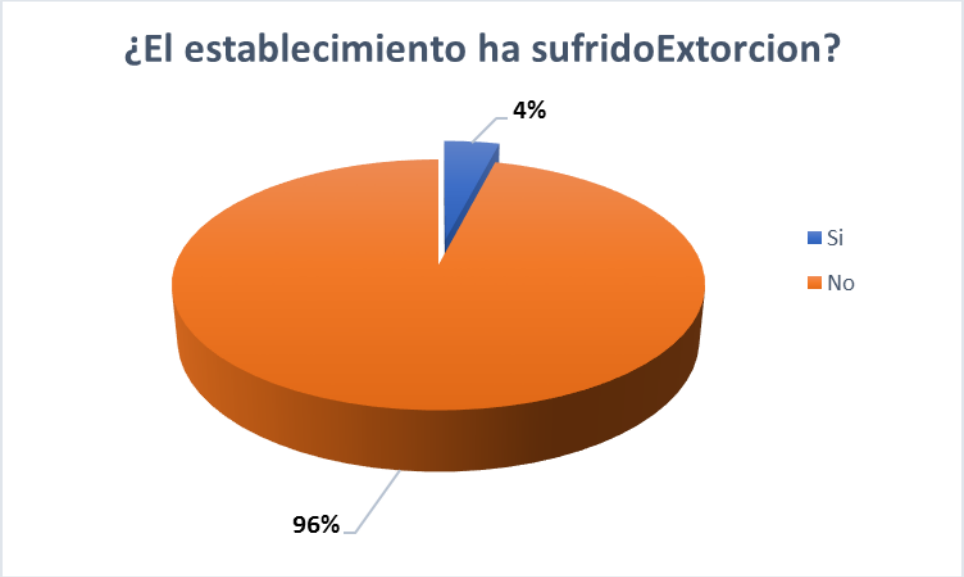
Estas son señales y lo más recomendable siempre es no hacer caso, ni entrar en los vínculos que aparezcan a menos que se conozca la persona o la institución que los envió, en muchos casos es recomendable utilizar en sus dispositivos móviles una VPN (Virtual Private Network) como puede ser Norton Secure VPN, de esta manera se pueden proteger y encriptar todos los datos que se pueden enviar o recibir mediante internet o incluso mensajes de texto para que resulten inaccesibles por parte de terceros que traten de interceptar la conexión.

5) **Extorsión**: En esta ocasión el delincuente pretende el pago en dinero efectivo o moneda virtual (bitcoins) afectando el patrimonio de su víctima, quien se encuentra bajo la amenaza de hacer públicas información sensible (fotos, videos, información personal, datos empresariales) que los ciberdelincuentes aseguran tener, el modus operandi en esta modalidad es “el uso de un software malicioso conocido como ransomware, este término proviene de las palabras del idioma inglés “ransom”, cuyo significado es rescate y “software”, programa de cómputo, normalmente cifra los archivos de la víctima para pedir un rescate por ellos. Recientemente, se ha observado

[40] INCIBE. *Smishing*. [en línea], 2020. [Consulta: 6 julio 2022]. Disponible en: https:// www.incibe.es/ciberseguridad/smishing.

que los ataques inician con correos electrónicos los llamados phishing anteriormente mencionados que contienen archivos maliciosos adjuntos, a su vez contienen otros archivos comprimidos con el mismo nombre y éste última aloja un binario que es el downloader[41]. Una vez que se ejecuta, abre un documento en Microsoft Word (incluido en el software malicioso) y se descarga el ransomware, que cifra archivos en el equipo comprometido y solicita el pago del rescate normalmente en bitcoins, depósitos a cuentas o incluso tarjetas prepago".

Grafico 19.



Fuente: Elaboracion Propia. Establecimientos comerciales del centro de la ciudad de León, departamento de León.

La extorsión por medios electrónicos en los últimos años ha causado que muchas empresas y usuarios estén actualizados en sus programas para proteger y codificar los softwares debido a que los extorsionistas tienen tácticas de intimidación como llamadas por teléfono, mensajes de texto o correos electrónicos donde muestran que conocen contraseñas que has utilizado para alguna cuenta en línea. En la mayoría de los casos afirman haber implantado softwares maliciosos, los

[41] CYnergia. *Extorsión a través de medios electrónicos.* [en línea], 2016. [Consulta: 8 julio 2022]. Disponible en: https://cynergia.mx/delitos-financieros-o-contra-del-patrimonio/extorsion-a-traves-de-medios-electronicos/.

llamados ransomware[42] que les permite capturar las pulsaciones del teclado, mirar a través de la cámara web y acumular evidencia de que, por ejemplo, frecuencias en sitios web para adultos, además afirman compartir la información con todos tus contactos u otra forma para extorsionar a las personas o empresas, a cambio de generalmente dinero en forma de criptomonedas como Bitcoin (BTC), Ethereum (ETH), Cardano (ADA) o Tether (USDT), puesto que al ser monedas descentralizadas son muy difíciles de rastrear, otra forma de extraer dinero es mediante el pago a cuentas bancarias en el extranjero.

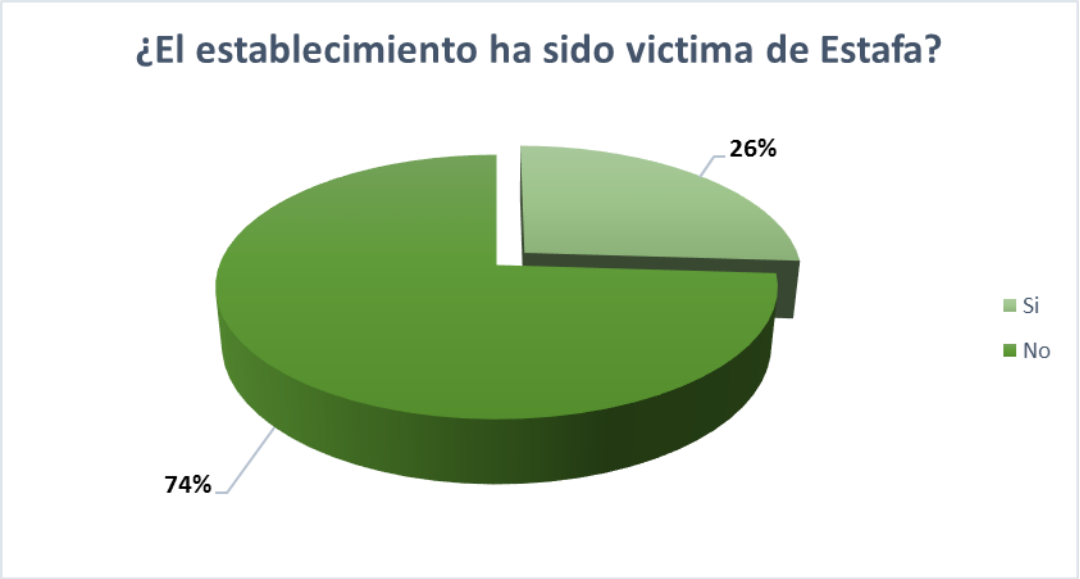
No obstante, hay pocas posibilidades de que el extorsionista cibernético realmente haya invadido tus cuentas y computadora, normalmente envían amenazas indiscriminadamente y usan grandes listas de direcciones de correos electrónicos, pero al responder el correo electrónico o pasar cierto tiempo en llamada con ellos si puede el Rasomware a trabajar, por eso es vital no responder a ninguna de estas amenazas.

En Nicaragua todavía no es una forma de ciberdelito muy conocida, ni utilizada, ya que el 96% de los establecimientos encuestados afirmaron nunca haber escuchado, ni tampoco haber sufrido de este nuevo modo de operar, sin embargo, a lo largo de Latinoamérica en los últimos 10 años se ha visto un incremento en la extorsión por medios electrónicos

6) **Estafas**: El analista Ignacio Acosta Sorge, define la estafa electrónica como "la comisión, con ánimos de lucro, de un acto que produzca daños y perjuicios patrimoniales cuantificables a terceros, cometido mediante el uso ilícito de tecnologías y procedimientos de la informática, es decir, cualquier transferencia no consentida de un activo patrimonial que produzca daños a terceras personas, mediante la manipulación indebida de la informática."

[42] AARP. *Estafas de extorsión por correo electrónico.* [en línea], 2019. [Consulta: 8 julio 2022]. Disponible en: https://www.aarp.org/estafas-y-fraudes/info-2019/extorsion-por-correo-electronico.html.

Grafico 20.



Fuente: Elaboracion Propia. Establecimientos comerciales del centro de la ciudad de León, departamento de León.

De la última década hasta nuestros días las empresas y entidades bancarias principalmente debido a que se han esforzado por simplificar la banca en línea y agilizar los pagos de los clientes antes los cambios que se vieron acelerados por la pandemia del COVID-19 en 2020 se ha visto el paulatino aumento de las estafas en todos sus ámbitos, ya que más personas están demandando hacer compras y pagos en línea.

Los estafadores no atacan a las entidades bancarias de manera directa, sino que les resulta más sencillo llegar a los usuarios de dichas instituciones, según nuestras encuestas el 74% de los establecimientos encuestados no han sufrido de ninguna forma de estafa por medios electrónicos pero la mayoría conocen de estas nuevas formas de sustracción de información y dinero, sin embargo, el 26% de los establecimientos han sufrido de estafas electrónicas ya sea a través de llamadas, por correo electrónico y lo más recientes fraudes a través de redes sociales.

Mediante correo electrónico, que es donde los defraudadores pueden recrear sitios web idénticos a una entidad bancaria y enviar enlaces a sus direcciones de correo que en cualquier momento pedirá sus datos de acceso e información personal[43].

A través de llamadas, es de las formas más fácil de cometer fraude pues consiste en un supuesto aviso del banco, que informa sobre un problema informático o movimientos inusuales en tus cuentas o tarjetas, normalmente la persona al otro lado de la línea utiliza similar protocolo de atención al cliente y en algunos casos hasta ponen de fondo música o mensajes publicitarios del banco.

Los estafadores piden que brindes tus datos de acceso bancario por "tu seguridad", así como credenciales para confirmar tu identidad y poder evitar un futuro robo, cuando el robo está en proceso realmente.

Y, por último, los más recientes fraudes que son a través de redes sociales, en donde promociones o sorteos desde perfiles que aparentan ser de instituciones bancarias, e incluso pagando publicidad, han sido identificadas como fraudes.

Lo primero que el usuario debe hacer para no ser una víctima más a la lista es conocer las plataformas que utilizan y hacer el uso correcto de las redes sociales puesto que aplicaciones como Facebook y Twitter permiten ver la fecha de creación de cada página o perfil, así como número de seguidores y restos de publicaciones, por lo que con una sola vista se puede saber si es un perfil oficial o no, igualmente los perfiles oficiales de las entidades bancarias aquí en Nicaragua cuentan con el "Check" de verificación de la cuenta, lo que evidencia que realmente es quienes dicen ser.

Otra forma de fraude que se está haciendo popular, sobre todo entre micro y pequeñas empresas o personas que venden directamente en las redes sociales es cuando son contactados por un supuesto comprador, generalmente del extranjero que desea comprar al por mayor el producto que se está ofreciendo y en el momento de realizar el pago, por medio de una transferencia electrónica aseguran tener inconvenientes y haber contactado al banco para verificar y hacen comunicación entre las tres partes para resolver el inconveniente pero realmente lo que sean es

[43] BAC CREDOMATIC. *Así operan las estafas estos días.* [en línea], 2022. [Consulta: 10 julio 2022]. Disponible en: https://www.baccredomatic.com/asi-operan-las-estafas.

que se les brinde información personal para acceder a la banca en línea y correo electrónico de los vendedores.

7) **Carta Nigeriana**: Esta modalidad es de las más antiguas de ciberdelito y aunque al día de hoy muchas personas la catalogan como un engaño ridículo, en Latinoamérica ha ocasionado pérdidas millonarias, se basa en ofrecer a la víctima ser el dueño de una cantidad considerable de dinero, el contacto se hace a través de correos electrónicos donde le indican a la víctima que debe consignar por adelantado un pago, a fin de entregarle el "la herencia o fortuna".

Grafico 22.

Fuente: Elaboracion Propia. Establecimientos comerciales del centro de la ciudad de León, departamento de León.

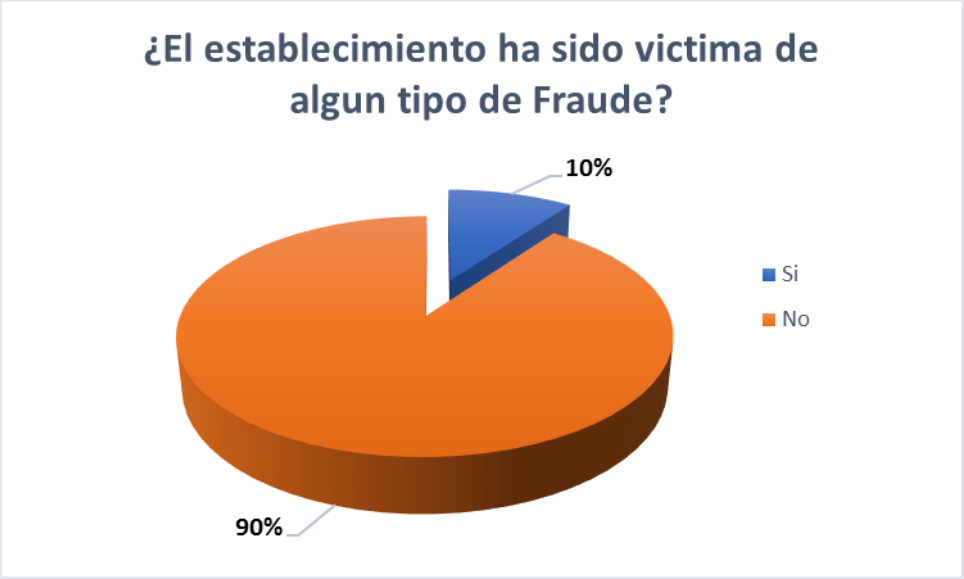
La Carta Nigeriana se podría decir que es la combinación entre la amenaza que ocasiona el Phishing y la extorsión pues los estafadores envían un correo electrónico originalmente desde Nigeria por eso el nombre de este tipo de fraude, sin embargo, ahora puede venir de cualquier parte del mundo, en el correo electrónico se le ofrece la oportunidad de ganar grandes cantidades de dinero en efectivo a cambio de una pequeña cantidad.

El autor de la Carta en la mayoría de los casos afirma ser un oficial del gobierno y trata de que la víctima le envié información personal, tal como papelería en blanco con membretes, nombres de bancos y números de cuentas bancarias, así como cualquier tipo de información personal.

El éxito de la Carta Nigeriana dependerá de convencer a la víctima para que esté dispuesta a enviar dinero al autor de dicha carta en forma de pagos parciales cada vez mayores y con motivos diversos[44].

En Nicaragua no es la excepción, ya que la Carta Nigeriana es de los fraudes más conocidos y que más afectan a la población en General, si bien en nuestras encuestas el 88% de los establecimientos no han sido víctimas de este tipo de fraude, si se admitió que todos los establecimientos han recibido en más de una ocasión correos o mensajes de textos en los cuales se les afirma haber sido ganadores de altas cantidades de dinero a cambio de cuotas, no obstante el 12% de los establecimiento encuestados que han sufrido este tipo de fraude afirman haber dado en muchas cuotas altas cantidades de dinero sin recibir ningún premio o fortuna.

Grafico 23.



Fuente: Elaboracion Propia. Establecimientos comerciales del centro de la ciudad de León, departamento de León.

Habiendo establecidos los tipos de fraudes más populares y usados que afectan las transacciones electrónicas en Nicaragua, el 10% de los encuestados afirmaron haber sufrido de otros tipos de

[44] FEDERAL BUREAU OF INVESTIGATION (FBI). *Fraude de Carta de Nigeria Sigue Defraudando.* [en línea], 2022. [Consulta: 10 julio 2022]. Disponible en: https://www.fbi.gov/news/espanol/fraude-de-carta-de-nigeria.

fraudes los cuales se desconocía, pero gracias a la participación de las personas y establecimiento se pudo conocer, entre ellos se encuentra el Pharming y el Sim Swapping.

El pharming es un tipo de fraude en línea que consiste en dirigir a las personas a páginas webs fraudulentas que imitan paginas auténticas, el pharming intentan convencer a las personas para interactuar con páginas web falsas y parecidas con el fin de recopilar datos personales y afectando a sus ordenadores con malware.

El pharming es similar al phishing, pero los fraudes cometidos de pharming proyectan redes muchos más amplias, avanzadas y complejas de descifrar y da una manera mucho más fácil de ser engañado por una versión falsa de una página web de confianza como la banca en línea de una entidad bancaria, redes sociales y páginas de internet que se pueden frecuentar.

Por otro lado, el Sim Swapping no es más que el duplicado de la tarjeta SIM del teléfono celular, sin embargo la mayoría de las cuentas bancarias actualmente y muchas información sensible requiere del número celular por lo que una copia de la tarjeta SIM crea un acceso directo a este tipo de información, a su vez es muy difícil evitar porque la copia se realizar por medio de un adaptador que puede encontrarse en cualquier punto donde se pueda conectar el teléfono celular, ya sea en un red wifi con malware.

3.2 Unidad de Análisis Financiero

La UAF (Unidad de Análisis Financiero) de Nicaragua es la encargada de fortalecer las alertas y así dirigir acciones a la prevención, disminución y erradicación de las estafas y ciberdelitos que se han comenzado a dar de manera más seguida y cada vez más difícil de descifrar en nuestro país.

la UAF realizo estudios durante el año 2021 donde se presentó un aumento significativo en donde evidentemente se aprovecharon de la pandemia del COVID-19, en la cual se destacada como el fraude más utilizado al Phishing con 44%, esto como resultado de acelerar el uso de

plataformas electrónicas[45]. Así mismo se dio un aumento de hasta el 36.6% en las denuncias por estafa en el año 2020 con respecto al año 2019, aunque no se especifica la modalidad utilizada.

Actualmente las instituciones financieras han optimizado los servicios ofertados a sus clientes, brindándoles mayores facilidades, comodidad, ahorro de tiempo y seguridad, por tanto, los clientes, en su mayoría, hacen un constante uso del Internet para ejecutar todo tipo de gestiones y transacciones financieras y comerciales que le son permitidas por esta vía, no obstante, es importante destacar que el riesgo a ser víctimas de la ciberdelincuencia aumenta, y se maximiza cuando existen estas prácticas insuficientes y falta de medidas de seguridad por parte de los usuarios en el uso de las tecnologías de la información y comunicación (TIC).

Por lo que, es un hecho que la mayoría de los usuarios del Internet al mantener en la nube una cantidad increíble de datos personales, así como, de parientes y de amistades, les permite a los ciberdelincuentes poder conocer previamente a sus potenciales víctimas, caracterizándolos con solo leer sus publicaciones en las diferentes redes sociales, además, de aquellos formularios que los mismos llenan en línea en la búsqueda de empleo o la oferta de bienes o servicios.

[45] UNIDAD DE ANÁLISIS FINANCIERO. “Guía Especial para la Prevención, Detección y Enfrentamiento a las Estafas y Ciberdelitos.” [en línea]. 2022 [Consulta: 10 julio 2022]. :Disponible en: https://www.uaf.gob.ni/images/Pdf/DocumentosGuia-UAF-Estafas-y-ciberdelitos-UV.pdf.

Diseño Metodológico

La presente investigación es de tipo mixto, ya que se emplearon métodos cuantitativo y cualitativo, para un estudio más completo y detallado, se recopilaron datos de fuentes documentales tales como leyes, libros, tesis, artículos científicos y/o cualquier otro tipo de documento gráfico, icnográfico y electrónico en su mayoría[46].De igual forma, se recopilaron y analizaron datos a través de encuestas. En el mismo sentido, se utilizó un método de análisis síntesis[47]**,**donde se realizó una separación de la parte de un todo con la finalidad de estudiarlas en forma individual para después efectuar la reunión racional de los elementos dispersos y analizarlos en su totalidad. El método comparativo se utilizó para analizar las particularidades del sujeto de estudio en relación con otros siguiendo este método de investigación, tanto el planteamiento del problema, la forma y las técnicas de recopilar datos, como el análisis y la explicación de sus resultados estuvieron encaminados hacia un mejor entendimiento del comportamiento del fenómeno que se estudió[48], la presente investigación es de corte transversal dado que fue una investigación observacional que analizó datos de variables recopiladas en un periodo de tiempo sobre una población muestra o subconjunto predefinido. Además, se empleó el método deductivo**,** sabiendo que se partió del marco general de cómo funcionan las transacciones electrónicas, así como también el análisis jurídico de las mismas y el tratamiento que se debe de tener cuando se enfrente a los diferentes tipos de fraudes con la finalidad de poder detectarlos antes que logren hacer algún daño y hacia lo particular cómo funcionan realmente las transacciones electrónicas en la sociedad.

Área de estudio y periodo de estudio

El área de estudio fueron los establecimientos comerciales del centro de la ciudad de león, departamento de león, Nicaragua, nuestra muestra fueron todos aquellos establecimientos comerciales que realizan transacciones electrónicas. Se hizo uso de muestro no probabilístico, dentro del cual fue el muestreo intencional o de conveniencia al aplicar las encuestas a los

[46] MUÑOZ RAZO, Carlos. *Como elaborar y asesorar una investigación de tesis*, 2da Ed. México, Pearson Educación, 2011, p.14.
[47]VILLABELLA ARMENGOL, Carlos. *La investigación y comunicación científica en la ciencia jurídica*, 1ra Ed. México, Instituto Mexicano de Ciencias Jurídicas de Puebla, 2009, p.37
[48] MUÑOZ RAZO, Carlos, *op.cit.*, p.23

establecimientos que cumplen con características de interés para la investigación, en un periodo de estudio de noviembre y diciembre del 2021.

Población de estudio

Los criterios de inclusión en la encuesta fueron los establecimientos que realizan transacciones electrónicas como una forma de servicio a sus consumidores en el centro de la ciudad de león, departamento de león, Nicaragua y los criterios de exclusión fueron todos los demás establecimientos no pertenecientes.

Técnica e instrumento de recolección de la información:

La recolección de información se realizó a través de encuestas, las cuales se le entregaron a los encargados o jefes de los establecimientos y seguidamente se les informo sobre los objetivos del estudio y la importancia de este, se solicitó la participación voluntaria de los establecimientos comprendidos en la muestra.

Sé les informo que era un estudio voluntario y que toda la información seria para fines académicos y que si no deseaban participar podían no hacerlo sin ninguna objeción, de igual forma brindamos instrucciones generales sobre el llenado del cuestionario, y reforzando paulatinamente, pregunta por pregunta, las orientaciones escritas que se les ofrecieron.

En el anexo 1 se adjuntan las encuestas propuestas, las cuales están estructuradas en preguntas cerradas

Confiabilidad y validez del instrumento

El cuestionario fue elaborado en consulta con el tutor de la monografía, lo que ha permitido realizarle mejoras.

Plan de análisis de los datos de la encuesta:

La base de datos y su procesamiento se realizó en el software IBM-SPSS versión 25. Se elaboraron tablas de frecuencia (absolutas y porcentajes) de cada una de las variables cualitativas (categóricas). Los resultados son presentados en forma tablas y/o gráficos.

Aspectos éticos:

Se les dio a conocer que toda la información brindada por ellos se mantendría de forma anónima ya que no se le solicitaron nombre o apellidos, también se le hizo saber a cada establecimiento que su participación fue voluntaria, teniendo el derecho a negarse o descontinuar de su participación en cualquier momento del estudio.

Conclusiones

1. Las transacciones electrónicas se han vuelto la forma principal de realizar comercio en todo el mundo después de la pandemia del covid-19.

2. La evolución de Internet influye ampliamente en el crecimiento y expansión del comercio electrónico en Nicaragua, las principales transacciones que se realizan en los establecimientos del municipio de león son: Las transacciones realizadas de negocio a consumidor (B2C), de negocio a empleados (B2E) y de negocio a negocio (B2B) siendo a través de transacciones a cuentas bancarias.

3. Aunque las transacciones electrónicas se utilizan de manera cotidiana y que en nuestra legislación existe un marco regulador para los fraudes cometidos a través medios electrónicos como la Ley de Protección de los Derechos de las Personas Consumidoras y Usuarias, Ley General de Bancos y otras Instituciones Financieras y la Norma sobre Gestión de Riesgo Tecnológico SIBOIF. Así mismo, para los ciberdelitos como la Ley 1042, Ley Especial de ciberdelitos, Internet se ha convertido en el espacio ideal para la ciberdelincuencia por el fácil acceso, anonimato, rápido flujo de información, altísimo impacto, escaso riesgos e indetectable.

4. Los fraudes electrónicos son una cadena de actos ilícitos que afectan de manera directa los bienes jurídicos del patrimonio e información personal, los fraudes mas recurrentes que afectan las transacciones electrónicas en León, Nicaragua son: Clonación de tarjetas de crédito/debito, Smishing, Estafa y Skimmin.

Recomendaciones

A. Establecer campañas de difusión e información sobre el comercio electrónico, dado que el estudio nos arrojó que son pocos los establecimientos que hacen uso de este tipo de comercio y aun menor el porcentaje de personas que conocen del comercio electrónico referido a sus beneficios como sus desventajas.

B. Hacer uso de las herramientas actuales a las que tenemos acceso, si bien el comercio electrónico está bien definido aún es una herramienta que seguirá evolucionando y del cual tenemos que sacar provecho.

C. Propuesta de reforma a la ley especial de ciberdelitos en donde se añadiría los tipos de fraudes informáticos para ser procesados de manera individual puesto que los bienes jurídicos tutelados no son los mismos en todos los fraudes.

D. Las Instituciones bancarias y establecimientos permanentes inviertan en Software que se encarguen de cifrar y encriptar la información confidencial y cuentas para así poder detectar y evitar el fraude en toda la medida de lo posible.

Fuentes del conocimiento

1. Disposiciones normativas citadas

CONSTITUCIÓN POLÍTICA DE LA REPÚBLICA DE NICARAGUA. Ultima Reforma en 2014.

GRAMM-LEACH-BLILEY ACT (GLBA). 1999.

LEY ESPECIAL DE CIBERDELITOS. Aprobada el 27 de octubre de 2020. Publicada en La Gaceta, Diario Oficial Nº. 201 del 30 de octubre de 2020.

LEY FEDERAL DE PROTECCIÓN AL CONSUMIDOR. Capítulo I Disposiciones Generales. [En Línea]. S.L.: Disponible En: https://www.profeco.gob.mx/juridico/pdf/l_lfpc_ultimo_camdip.pdf

LEY No. 561. LEY GENERAL DE BANCOS, INSTITUCIONES FINANCIERAS NO BANCARIAS Y GRUPOS FINANCIEROS. Publicada en la Gaceta No. 232 del 30 de noviembre de 2005.

LEY Nº. 842. *LEY DE PROTECCIÓN DE LOS DERECHOS DE LAS PERSONAS CONSUMIDORAS Y USUARIAS*. Aprobada el 13 de junio de 2013. Publicada en La Gaceta, Diario Oficial Nº. 129 del 11 de julio de 2013.

NORMA SOBRE GESTIÓN DE RIESGO TECNOLÓGICO. Resolución Nº CD-SIBOIF-500-1-SEP19-2007 De fecha 19 de septiembre de 2007.

2. Referencia Bibliográficas

AARP. *Estafas de extorsión por correo electrónico.* [en línea], 2019. [Consulta: 8 julio 2022]. Disponible en: https://www.aarp.org/estafas-y-fraudes/info-2019/extorsion-por-correo-electronico.html.

BAC CREDOMATIC. *Así operan las estafas estos días.* [en línea], 2022. [Consulta: 10 julio 2022]. Disponible en: https://www.baccredomatic.com/asi-operan-las-estafas.

BÁEZ GADEA, Juan Abel, TREJOS ALVARADO, Marvin Antonio, Tesis para licenciatura "Comercio electrónico de consumidor a consumidor". Universidad Nacional Autónoma de Nicaragua, Managua. 2016. Disponible en: https://repositorio.unan.edu.ni/9583/1/17175.pdf.

BELCIC, I., 2020. *¿Qué es un Sniffer y cómo puede protegerse?* [en línea]. [Consulta: 15 de febrero 2022]. Disponible en: https://www.avast.com/es-es/c-sniffer.

CABANELLAS, Guillermo, *Diccionario jurídico elemental*, duodécima edición, editorial Heliasta, 1998, p.76.

CERTIMATCH CONFIANZA DIGITAL, 2022. ¿Qué es el derecho informático y porqué es importante conocerlo? - CertiMatch. *CertiMatch* [en línea]. [Consulta: 21 julio 2022]. Disponible en: https://certimatch.com.mx/que-es-el-derecho-informatico-y-porque-es-importante-conocerlo/.

CYnergia. *Extorsión a través de medios electrónicos.* [en línea], 2016. [Consulta: 8 julio 2022]. Disponible en: https://cynergia.mx/delitos-financieros-o-contra-del-patrimonio/extorsion-a-traves-de-medios-electronicos/

Derecho Informático | Carlos Felipe Law Firm. *Fc-abogados.com* [en línea], 2022. [Consulta: 21 julio 2022]. Disponible en: https://fc-abogados.com/es/el-derecho-informatico-y-su-alcalce-regulador/.

El Comercio electrónico en Centroamérica - Consortium Legal. Consortium Legal [en línea], 2020. [Consulta: 17 marzo 2022]. Disponible en: https://consortiumlegal.com/el-comercio-electronico-en-centroamerica/.

FEDERAL BUREAU OF INVESTIGATION (FBI). *Fraude de Carta de Nigeria Sigue Defraudando.* [en línea], 2022. [Consulta: 10 julio 2022]. Disponible en: https://www.fbi.gov/news/espanol/fraude-de-carta-de-nigeria.

GAYA, ROMINA. "El comercio electrónico y la inserción internacional de América Latina y el Caribe" [En línea]. Buenos Aires. Argentina. 2020. [Consultado 5 de octubre del año 2021.] Disponible en: https://conexionintal.iadb.org/2015/10/15/el-comercio-electronico-y-la-insercion-internacional-de-america-latina-y-el-caribe/.

Historia de Internet: *¿cómo nació y cuál fue su evolución? Marketing for Ecommerce* -revista de marketing e-commerce [en línea], 2021. [Consultado 3 de marzo del 2022]. Disponible en: https://marketing4ecommerce.net/historia-de-internet/#:~:text=%C2%BFCu%C3%A1ndo%20naci%C3%B3%20Internet%3F%20(al,as%C3%AD%20la%20red%20Arpa%20Internet.

INCIBE. *Smishing*. [en línea], 2020. [Consulta: 6 julio 2022]. Disponible en: https:// www.incibe.es/ciberseguridad/smishing

LOAISIGA MENDOZA, Eva Julia, LÓPEZ CASTILLO, Darling María, LÓPEZ PÉREZ, Félix Rafael. Tesis para licenciatura "ANÁLISIS DEL DERECHO DE LOS CONSUMIDORES CON RELACION AL USO DEL COMERCIO ELECTRONICO EN NICARAGUA". Universidad Nacional Autónoma de Nicaragua, León. 2017. Disponible en http://riul.unanleon.edu.ni:8080/jspui/bitstream/123456789/6675/1/238966.pdf.

MALWAREBYTES, 2018. Spyware. *Malwarebytes* [en línea]. [Consulta: 12 febrero 2022]. Disponible en: https://es.malwarebytes.com/spyware.

MARIN, RODOLFO. *¿Qué son las terminales POS y cómo ayudan a los comercios? BBVA NOTICIAS* [en línea]. 2020. [Consulta: 5 julio 2022]. Disponible en: https://www.bbva.com/es/ar/que-son-las-terminales-pos-y-los-comercios/.

MICROSOFT. What Is Phishing, 2022. *Protéjase del phishing*. [en línea]. [Consulta: 5 julio 2022]. Disponible en: https://support.microsoft.com/es-es/windows/-phishing-ataque.

MONROY, P., 2021. ¿Qué es el Derecho informático? *Soycest.mx* [en línea]. [Consulta: 21 julio 2022]. Disponible en: https://www.soycest.mx/blog/index.php/derecho-informatico.

MUÑOZ RAZO, Carlos. *Como elaborar y asesorar una investigación de tesis*, 2da Ed. México, Pearson Educación, 2011, p.14.

OLIVERA, Noemí "Reflexiones e n Torno al sistema Jurídico de la Sociedad de la Información. LL UNLP 2008

OMC. *Comercio electrónico*. *Wto.org* [en línea], 2022. [Consulta: 3 marzo 2022]. Disponible en: https://www.wto.org/spanish/thewto_s/whatis_s/tif_s/bey4_s.htm.

ORGAZ, Cristina J. *"Prevenir que te clonen la tarjeta bancaria y te roben tus datos".* 29 de mayo del 2019. [Consulta: 5 julio 2022]. Disponible en: https://www.bbc.com/mundo/noticias-48433105.

SALAS PEÑA, DANIELA. "Responsabilidad civil bancaria frente al cliente por delitos informáticos" [En línea], Tesis de licenciatura, Universidad de Costa Rica, Costa Rica, 2010. P.242. Disponible en:http://iij.ucr.ac.cr/wp-content/uploads/bsk-pdf-manager/2017/06/Tesis-Daniela-Salas.pdf.

SÁNCHEZ MEDERO, Gemma. *"Delitos en internet: clases de fraudes y estafas y las medidas para prevenirlos*". Madrid. 2012.

UNIDAD DE ANÁLISIS FINANCIERO. "Guía Especial para la Prevención, Detección y Enfrentamiento a las Estafas y Ciberdelitos." [en línea]. 2022 [Consulta: 10 julio 2022]. :Disponible en: https://www.uaf.gob.ni/images/Pdf/DocumentosGuia-UAF-Estafas-y-ciberdelitos-UV.pdf.

UTEL Universidad. BLOG | UTEL [en línea], 2017. [Consulta: 2 March 2022]. Disponible en: https://utel.edu.mx/blog/menu-profesional/facultad-de-economia-y-administracion/comercio-internacional-desde-el-trueque-hasta-el-e-commerce/.

VILLABELLA ARMENGOL, Carlos. *La investigación y comunicación científica en la ciencia jurídica*, 1ra Ed. México, Instituto Mexicano de Ciencias Jurídicas de Puebla, 2009, p.37.

Anexo

Universidad Nacional Autónoma de Nicaragua
UNAN León

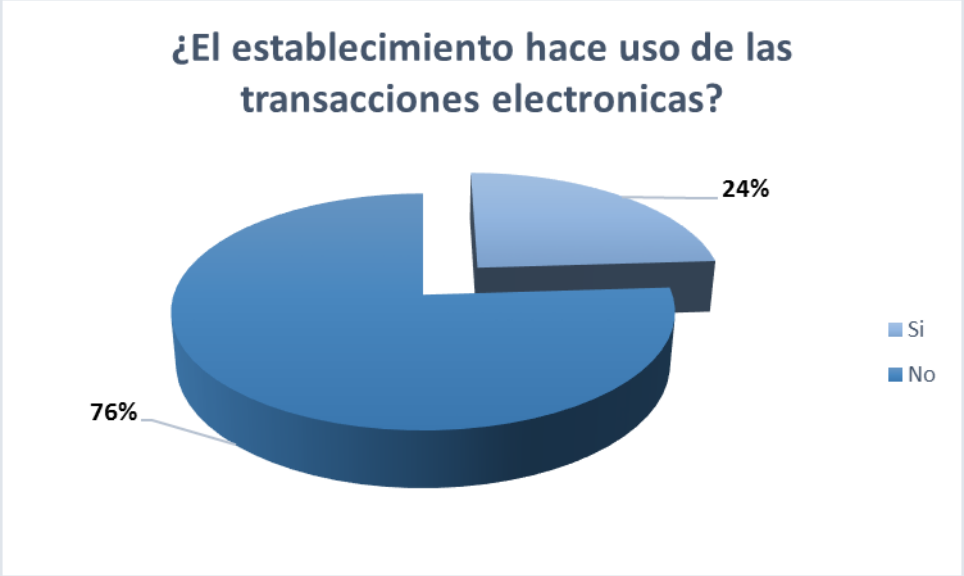
Objetivo: Señalar las diferentes transacciones electrónicas e Identificar los tipos de fraudes que se presentan en las mismas en Nicaragua

SECCIÓN I. ASPECTOS SOBRE LAS TRANSACCIONES ELECTRONICAS		
1	¿El establecimiento hace uso de transacciones electrónicas?	• Si • No
2	¿por qué usted no haría uso de las transacciones electrónicas en su establecimiento?	• No se sienten seguros de este método • Si hace uso
3	¿El establecimiento tiene conocimientos sobre el uso de las transacciones electrónicas?	• Si tiene conocimiento • No tiene conocimiento
4	¿El establecimiento da capacitación sobre el uso de las transacciones electrónicas?	• Si da capacitación • No da capacitación
5	¿El establecimiento realiza transacciones Empresa y Empresa (B2B)?	• Si • No
6	¿El establecimiento realiza transacciones Empresa y consumidor(B2C)?	• Si • No
7	¿El establecimiento realiza transacciones Empresa y empleados (B2E)?	• Si • No
8	¿El establecimiento realiza transacciones consumidor y consumidor (C2C)?	• Si • No
9	¿El establecimiento realiza transacciones Gobierno y consumidor (G2C)?	• Si • No
1	¿Con cuanta frecuencia el establecimiento hizo uso de las transacciones electrónicas en año 2021?	• Nunca • A veces • Frecuentemente • Siempre
1	¿Es política del establecimiento ofrecer dentro de sus servicios las transacciones electrónicas?	• Si • No

1	¿El establecimiento cuenta con un seguro en caso de fraude en las transacciones electrónicas?	• Si • No
1	¿El establecimiento cuenta con un protocolo para proceder en caso de Fraude en las transacciones electrónicas?	• Si • No
1	¿El establecimiento siente seguridad en el comercio electrónico?	• Si • No
1	¿Por qué no sentiría seguridad con este tipo de comercio?	• Falta de regulación • Falta de tecnología • Otro
1	¿Cuáles son las ventajas que le ofrece el comercio electrónico a su establecimiento?	• Disponibilidad 24-7 • Accesibilidad desde cualquier lugar • Ahorro de costes • Mayor acceso a clientes • Otras
SECCIÓN III. FRAUDE ELECTRONICO O INFORMATICO		
	¿El establecimiento ha sufrido Skimmin (robo de información mediante la copia de la banda magnética de la tarjeta de crédito)?	• Si •.....No
	¿El establecimiento ha sufrido clonación de Tarjetas?	• Si •.....No
	¿El establecimiento ha sufrido Smishing (pretenden suplantar la identidad, a menudo de personal bancario o establecimientos comerciales, con el fin de que las personas accedan mediante mensaje de texto o llamada a un link que le proporcionara al atacante información necesaria para hackear el teléfono de la víctima)?	• Si •.....No
	¿El establecimiento ha sufrido Extorsión (pretende el pago en dinero efectivo bajo la amenaza de hacer públicas informaciones sensibles)?	• Si •.....No
	¿El establecimiento ha sufrido Estafa (cualquier transferencia no consentida)?	• Si •.....No
	¿El establecimiento ha sufrido Suplantación de identidad (Phising) (obtener contraseñas, claves de tarjetas de crédito, información financiera, entre otros, utilizando páginas webs falsas a las cuales dirigen a la víctima)?	• Si •.....No
	¿El establecimiento ha sufrido Carta	• Si •.....No

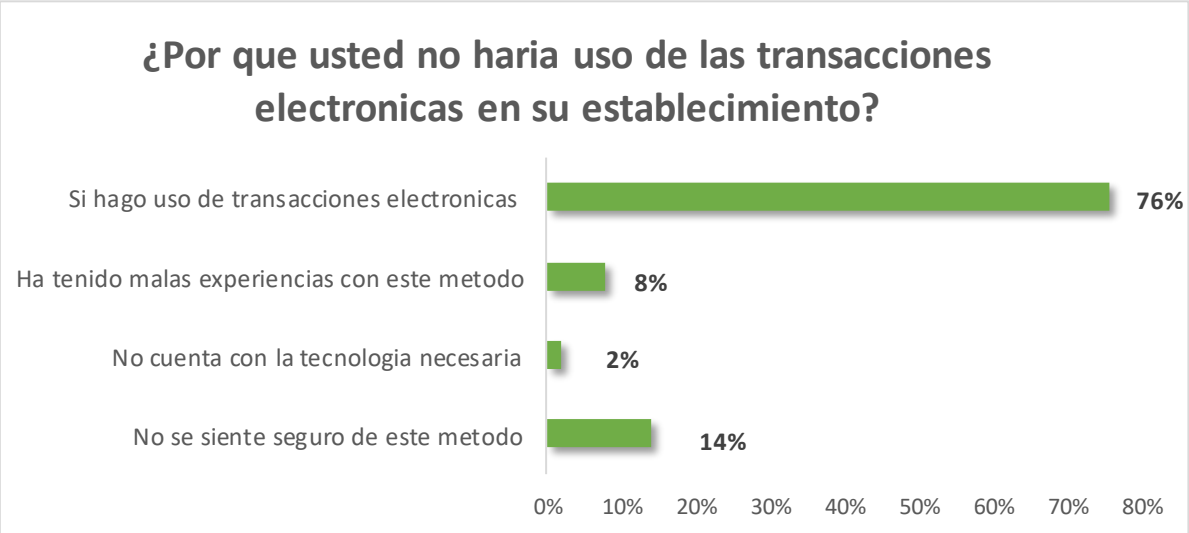
	Nigeriana (Esta modalidad ofrece a la víctima ser la dueña de una cantidad considerable de dinero, pero debe hacer un pago por adelantado, a fin de entregarle el dinero u objeto)?	
	¿El establecimiento ha sufrido algún otro tipo de fraude?	• Si •.....No

Gráfico 1.



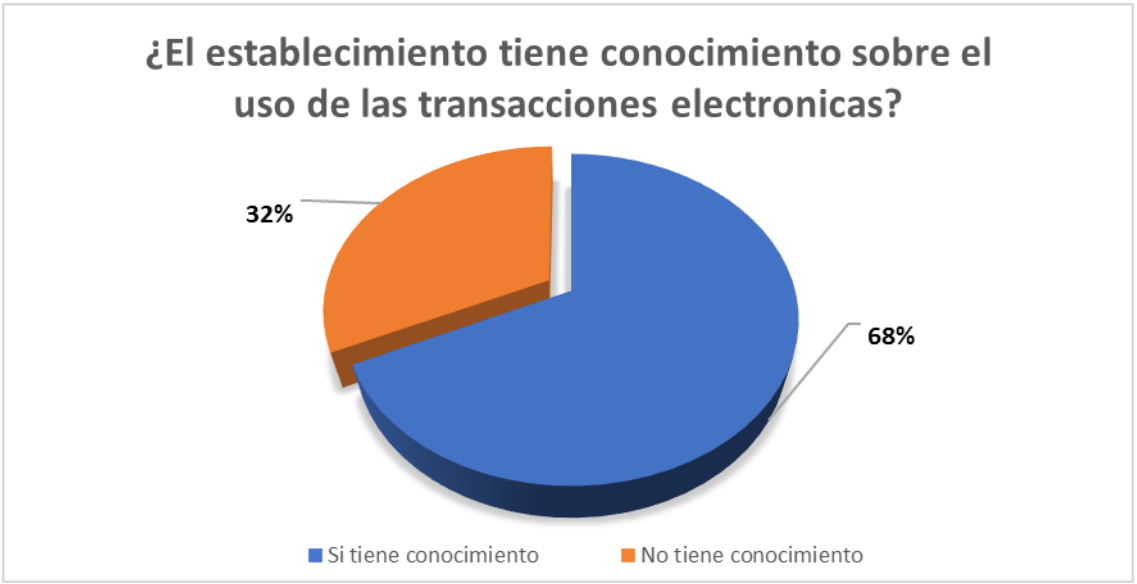
Fuente: Elaboracion Propia. Establecimientos comerciales del centro de la ciudad de León, departamento de León.

Gráfico 2.



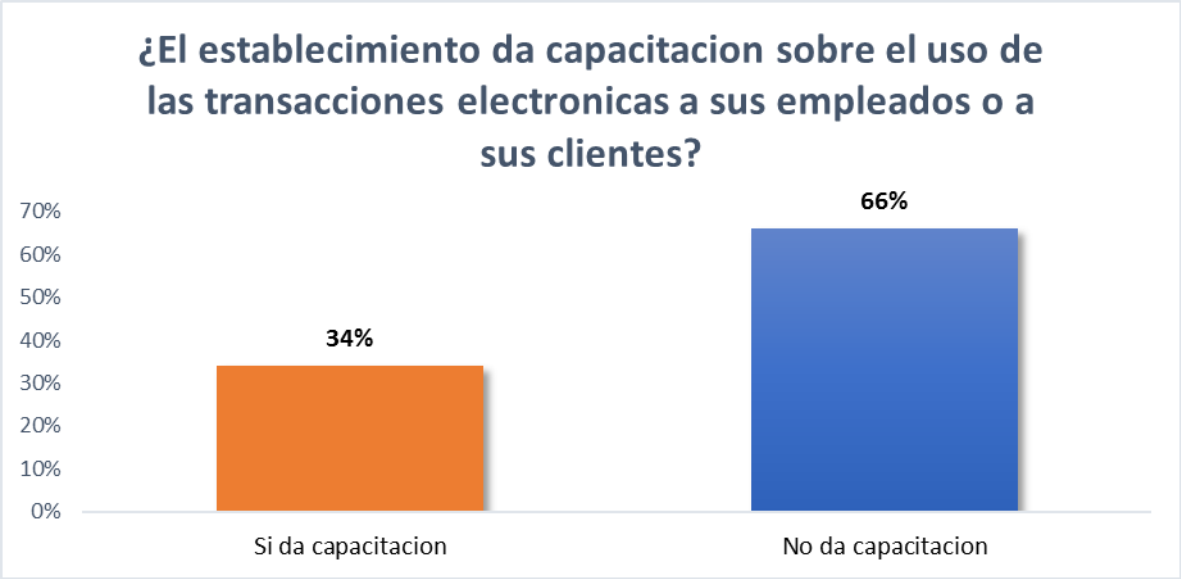
Fuente: Elaboracion Propia. Establecimientos comerciales del centro de la ciudad de León, departamento de León.

Gráfico 3.



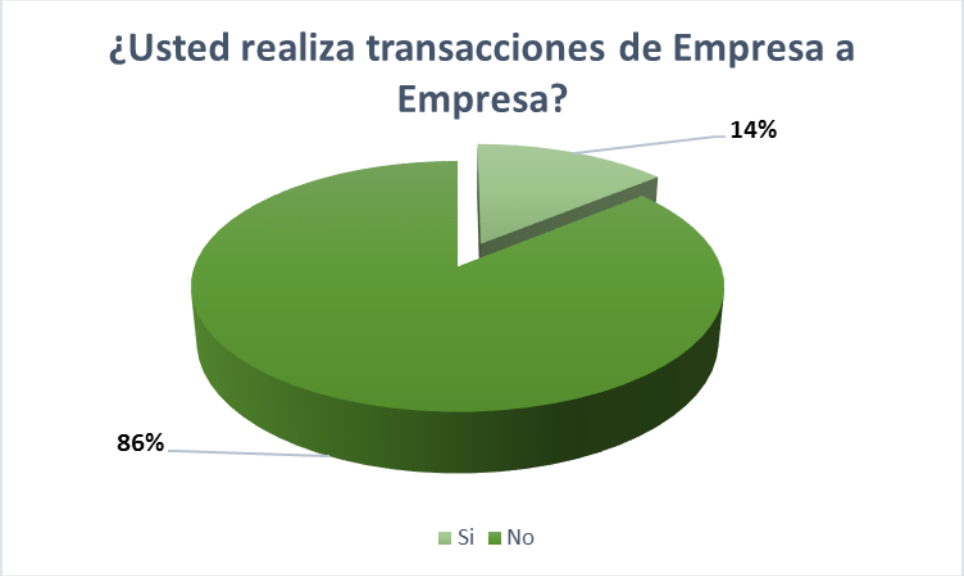
Fuente: Elaboracion Propia. Establecimientos comerciales del centro de la ciudad de León, departamento de León.

Gráfico 4.



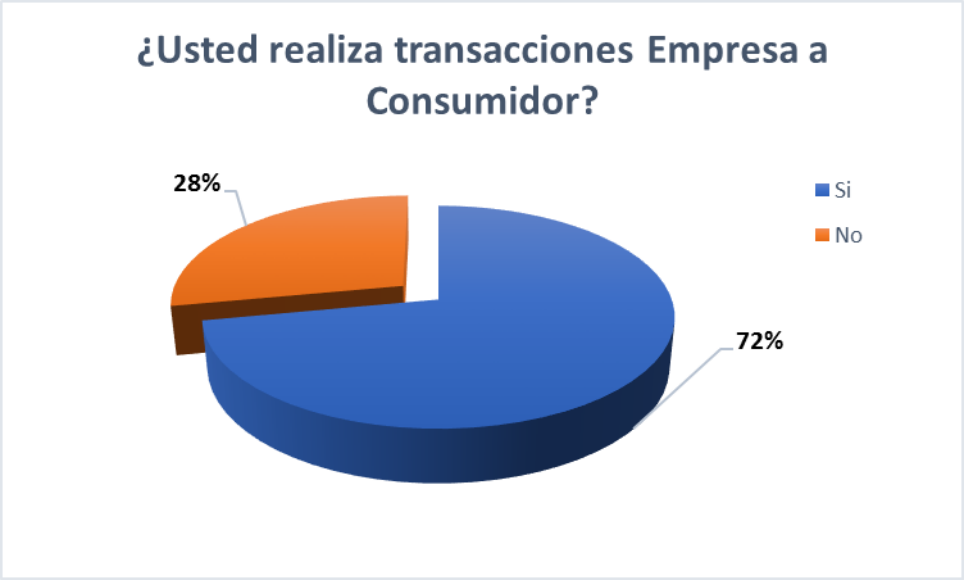
Fuente: Elaboracion Propia. Establecimientos comerciales del centro de la ciudad de León, departamento de León.

Grafico 5.



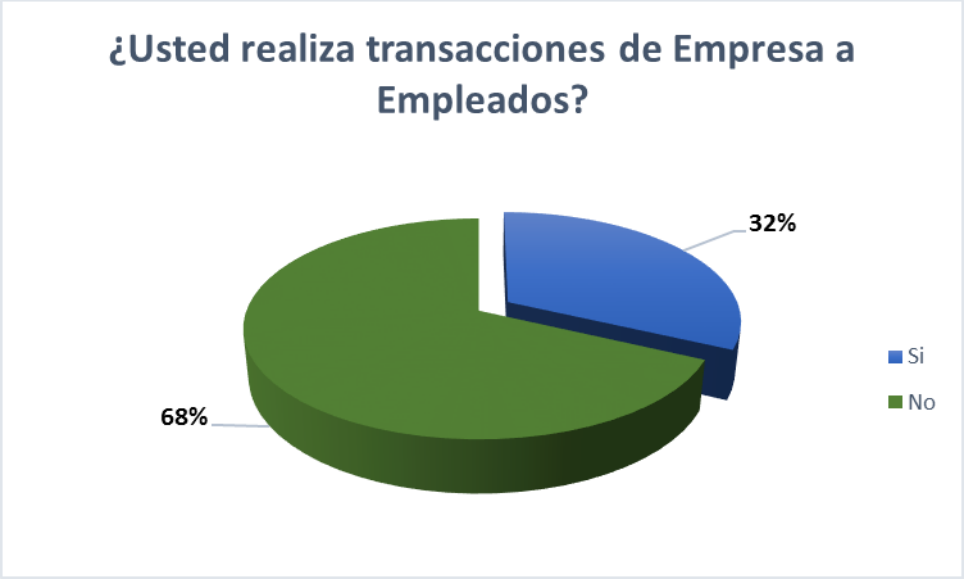
Fuente: Elaboracion Propia. Establecimientos comerciales del centro de la ciudad de León, departamento de León.

Gráfico 6.



Fuente: Elaboracion Propia. Establecimientos comerciales del centro de la ciudad de León, departamento de León.

Grafico. 7

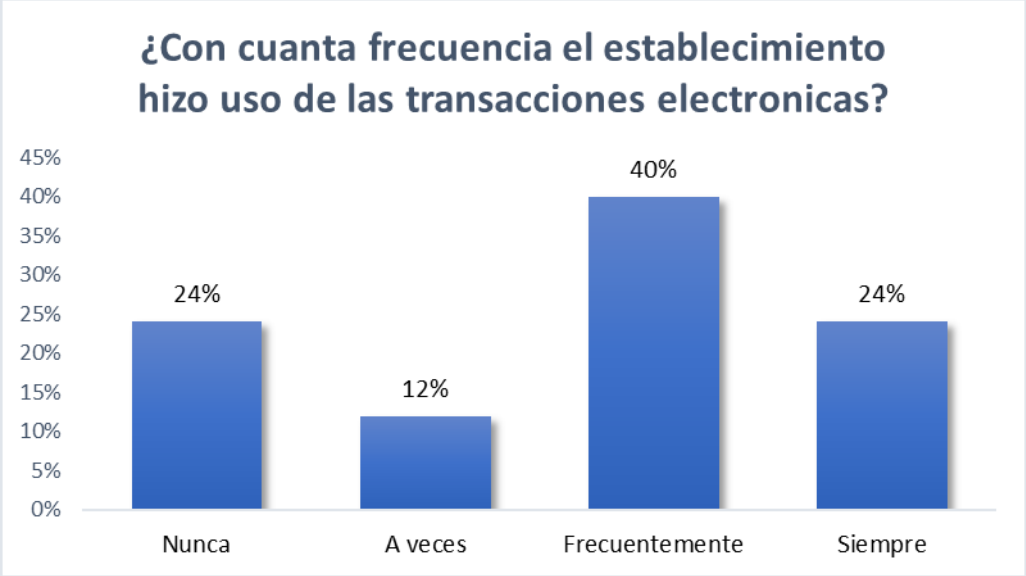


Fuente: Elaboracion Propia. Establecimientos comerciales del centro de la ciudad de León, departamento de León.

Grafico. 8.

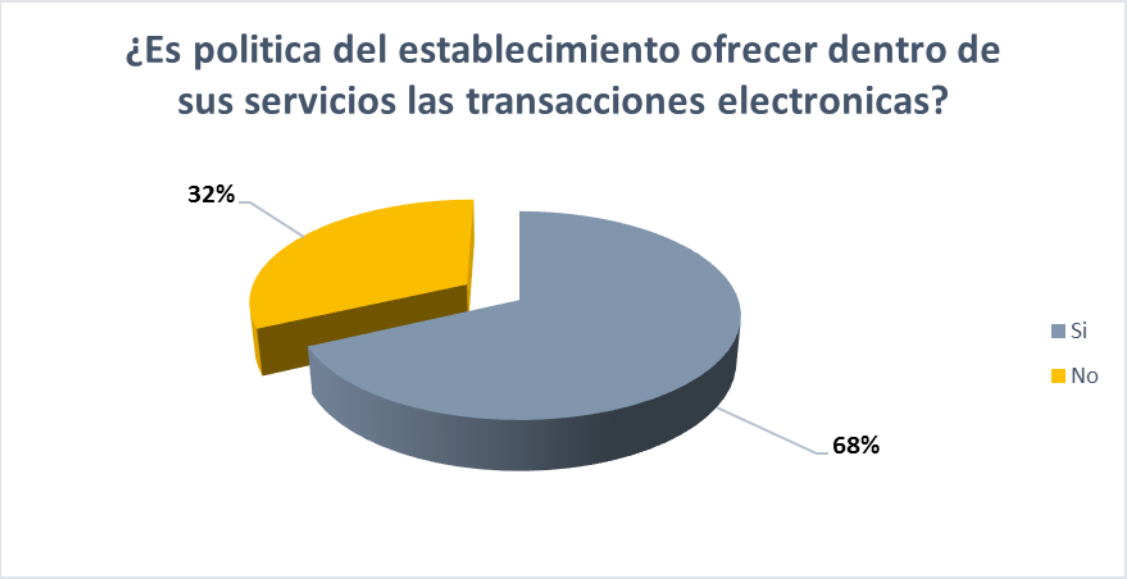
Fuente: Elaboracion Propia. Establecimientos comerciales del centro de la ciudad de León, departamento de León.

Gráfico 9.



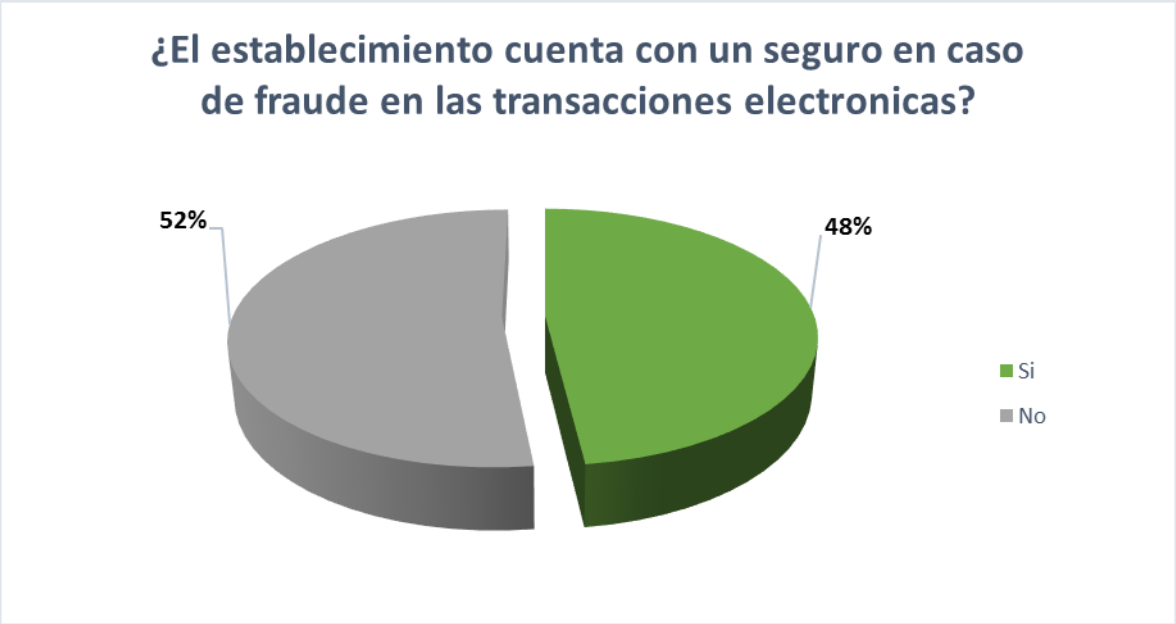
Fuente: Elaboracion Propia. Establecimientos comerciales del centro de la ciudad de León, departamento de León.

Gráfico 10.



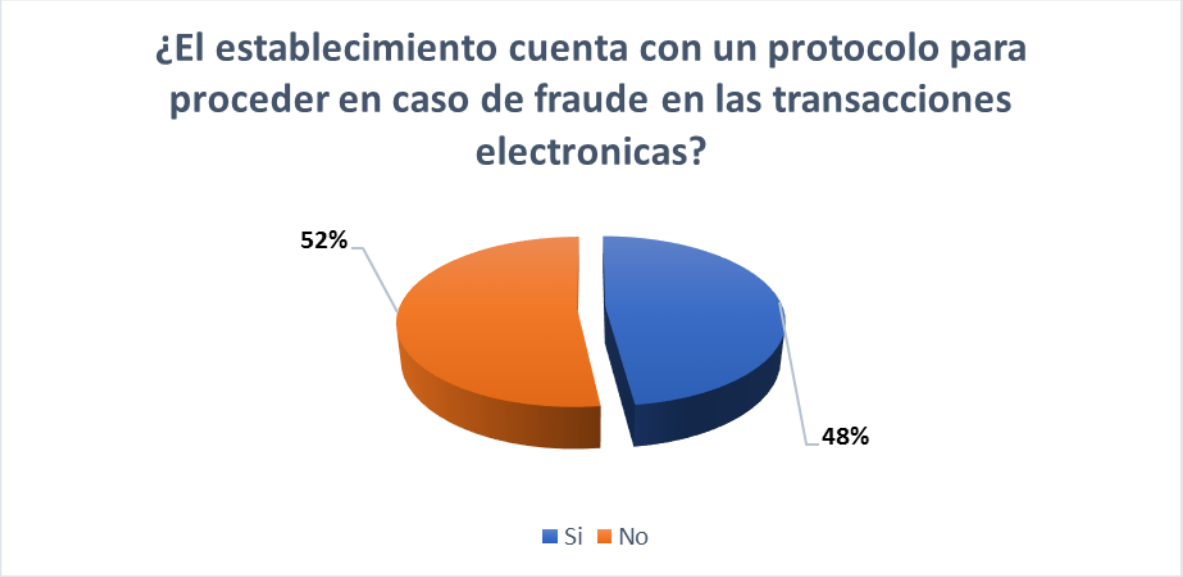
Fuente: Elaboracion Propia. Establecimientos comerciales del centro de la ciudad de León, departamento de León.

Gráfico 11.



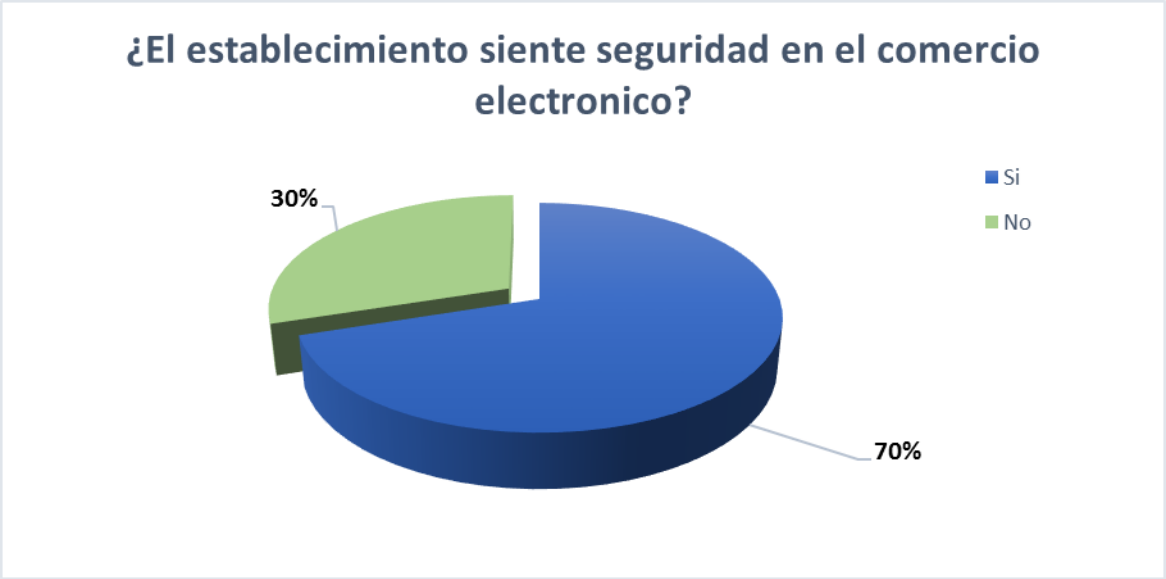
Fuente: Elaboracion Propia. Establecimientos comerciales del centro de la ciudad de León, departamento de León.

Grafico 12.



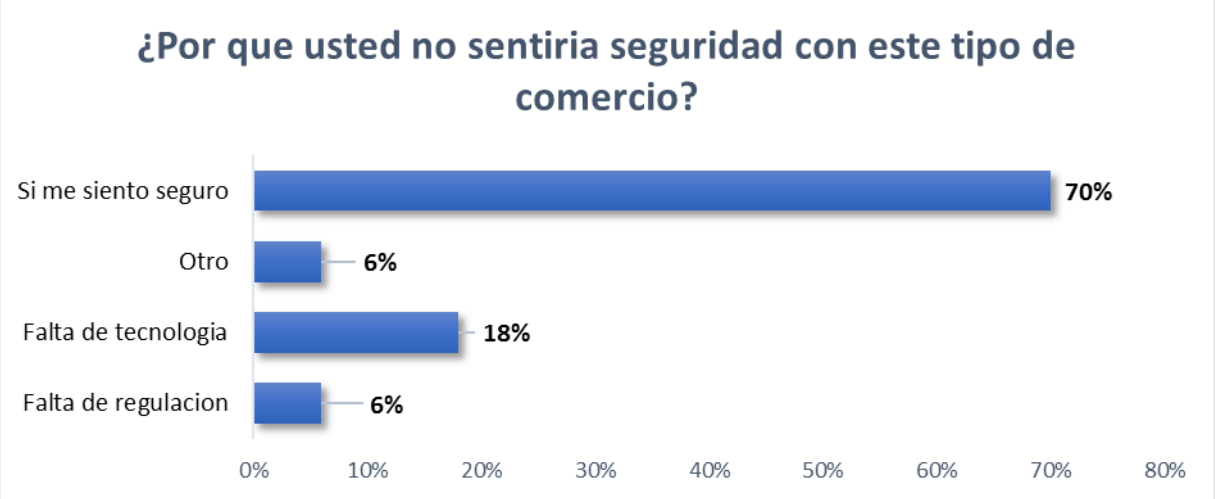
Fuente: Elaboracion Propia. Establecimientos comerciales del centro de la ciudad de León, departamento de León.

Gráfico 13.



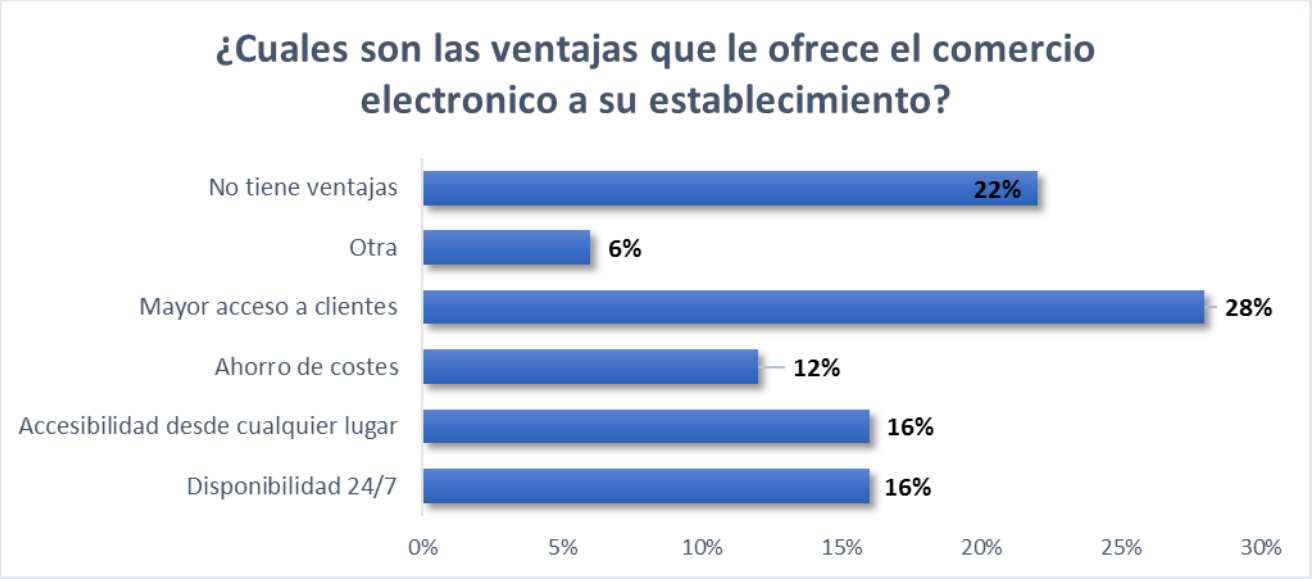
Fuente: Elaboracion Propia. Establecimientos comerciales del centro de la ciudad de León, departamento de León.

Gráfico 14.



Fuente: Elaboracion Propia. Establecimientos comerciales del centro de la ciudad de León, departamento de León.

Gráfico 15.

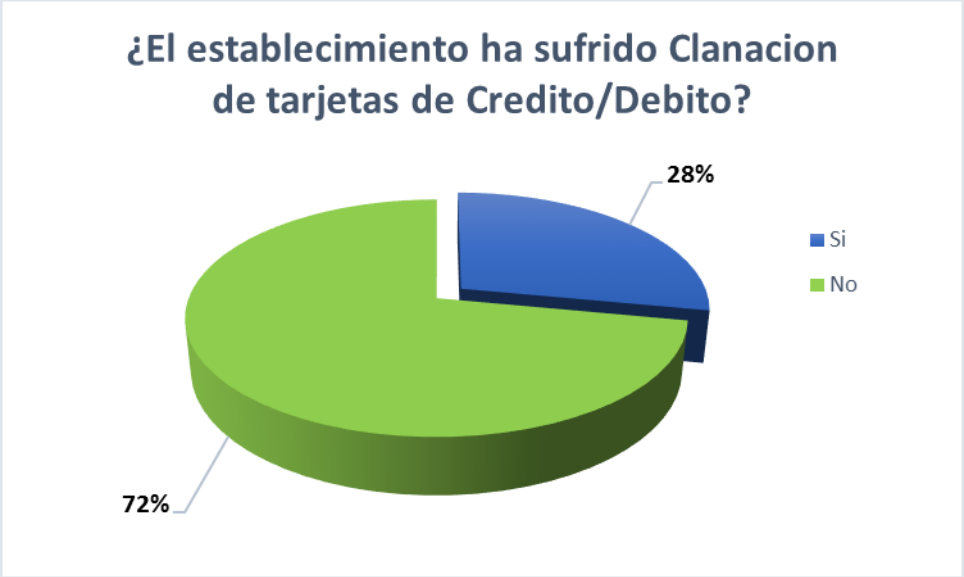


Fuente: Elaboracion Propia. Establecimientos comerciales del centro de la ciudad de León, departamento de León.

Grafico 16.

Fuente: Elaboracion Propia. Establecimientos comerciales del centro de la ciudad de León, departamento de León.

Gráfico 17.

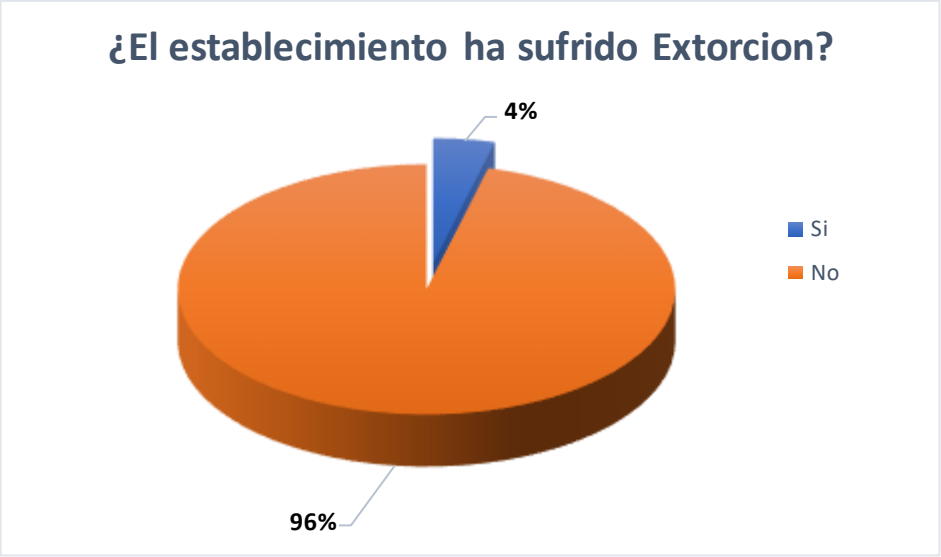


Fuente: Elaboracion Propia. Establecimientos comerciales del centro de la ciudad de León, departamento de León.

Gráfico 18.

Fuente: Elaboracion Propia. Establecimientos comerciales del centro de la ciudad de León, departamento de León.

Grafico 19.



Fuente: Elaboracion Propia. Establecimientos comerciales del centro de la ciudad de León, departamento de León.

Gráfico 20.

Fuente: Elaboracion Propia. Establecimientos comerciales del centro de la ciudad de León, departamento de León.

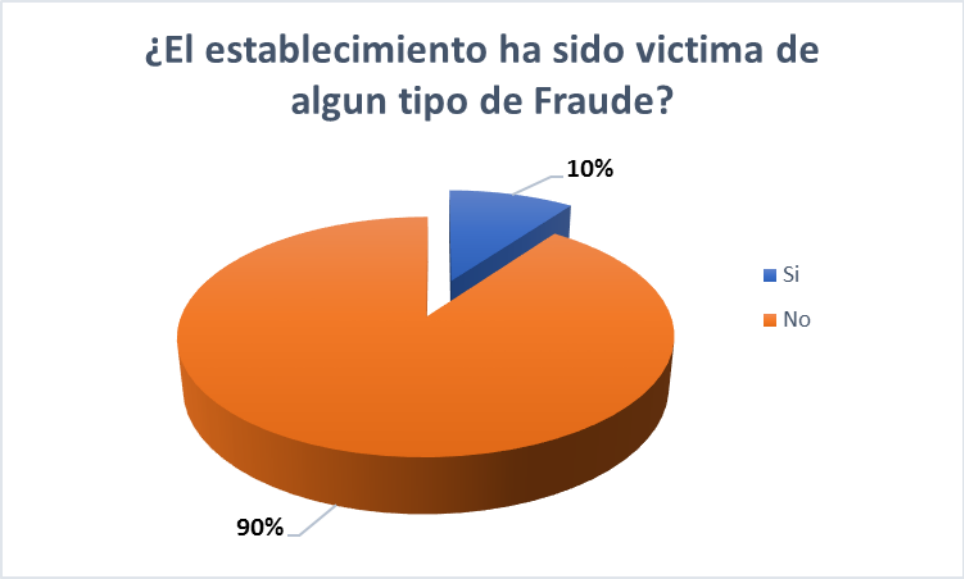
Gráfico 21.

Fuente: Elaboracion Propia. Establecimientos comerciales del centro de la ciudad de León, departamento de León.

Gráfico 22.

Fuente: Elaboracion Propia. Establecimientos comerciales del centro de la ciudad de León, departamento de León.

Gráfico 23.



Fuente: Elaboracion Propia. Establecimientos comerciales del centro de la ciudad de León, departamento de León.