



Vulnerabilidades orientadas a clientes de e-commerce y su impacto a raíz de la pandemia COVID-19.

Juan Felipe Castillo Moreno.

Luisa Fernanda Merchán Sánchez.

Trabajo de grado presentado como requisito para optar al título de:

Especialista en Seguridad de la Información.

Fundación Universitaria Los Libertadores.

Facultad de Ingeniería y Ciencias Básicas.

Bogotá, Colombia.

2021

Dedicatoria

A Dios por darnos la inteligencia, constancia, dedicación y paciencia para ejecutar este proyecto, por los triunfos y momentos difíciles que nos han dado valiosas lecciones para seguir adelante con nuestras vidas.

A nuestros padres por velar por nuestro bienestar y brindarnos lo mejor de sí para nuestro crecimiento personal, académico y profesional, su apoyo y confianza siempre serán el motor de nuestras vidas día a día.

A nuestros compañeros y docentes de la Fundación Universitaria Los Libertadores por su enseñanza, compromiso y empeño para que diéramos lo mejor de nosotros mismos a lo largo de la carrera y por hacer posible que alcancemos tan importante logro.

“No basta tener un buen ingenio, lo principal es aplicarlo bien”. René Descartes.

Tabla de contenido

Resumen.	4
Introducción.	5
Planteamiento del problema.	8
Objetivos.	9
Metodología.	10
Justificación.	11
Comercio electrónico en Colombia.	13
Tipos de comercio electrónico.	14
Business-to-Business (B2B) Negocio a Negocio	14
Business to Consumer (B2C) Negocio a Cliente	14
Business to Employee (B2E) Negocio a Empleado	15
Consumer to Business (C2B) Cliente a Negocio	15
Consumer to Consumer (C2C) Cliente a Cliente	15
Government to Consumer (G2C) Gobierno a Cliente	16
Pasarelas de pago.	16
Marco normativo y regulatorio.	18
Vulnerabilidades asociadas al comercio en línea.	24
Web Skimming	25
Ingeniería Social	26
Spear phishing	26
Defacement	27
Falsos QR	28
Robo de Identidad	28

Fraude de triangulación	28
Fraude de identidad comercial	30
Smishing	31
Vishing	32
Desarrollo Proyecto y Análisis de datos.	33
Conclusiones y Recomendaciones generales para evitar la explotación de las vulnerabilidades y disminuir el riesgo de incurrir en fraude.	19
Referencias.	53

Tabla de figuras.

<i>Radiografía de las pasarelas de pago en línea en Colombia.</i>	7
<i>Enfoque de los comercios e iniciativas presentadas para mejorar el entorno de pagos digitales.</i>	22
<i>Ejemplo Web Skimming.</i>	26
<i>Ejemplo Ingeniería Social.</i>	26
<i>Ejemplo de Spear Phishing.</i>	27
<i>Ejemplo Defacement.</i>	27
<i>Ejemplo Falsos QR.</i>	28
<i>Ejemplo Robo de identidad</i>	29
<i>Ejemplo Fraude de triangulación.</i>	29
<i>Ejemplo Fraude de Identidad Comercial.</i>	31
<i>Ejemplo Smishing</i>	32
<i>Ejemplo Vishing</i>	32

Resumen

La pandemia COVID-19 ha causado un impacto significativo en todos los sectores de la industria y la sociedad afectando la economía mundial y siendo un nuevo punto de partida en la sociedad, este impacto ha repercutido en el proceso y cambio en el comportamiento de las compras en línea y el crecimiento masivo de los servicios e-commerce; obligando a las empresas a replantear sus procesos de venta y forma de hacer negocios utilizando las diferentes herramientas tecnológicas y digitales de la mano con la conectividad hacia Internet y el acceso a redes de datos.

Es por esto, que el comercio electrónico o e-commerce toma mayor protagonismo a la hora de realizar procesos de compra; ya que al verse limitado el aforo de personas y el acceso físico a los establecimientos comerciales es necesario optar por mecanismos rápidos y seguros, además que los hábitos de compra y la dinámica de consumo cambiaron de forma significativa, por lo tanto esta situación trajo consigo una digitalización acelerada y exponencial de ahí que las pasarelas de pago sean las herramientas intermedias principales para la interacción entre empresas y consumidores.

Sin embargo, el comercio electrónico no está exento de vulnerabilidades, principalmente cibernéticas, ya que han ido en aumento a la par con el incremento de las compras en línea, de ahí que sea de gran importancia sensibilizar a los consumidores sobre las tendencias en ciberseguridad y regulación para el comercio electrónico y las pasarelas de pago brindando así un nivel de concienciación adecuado a la hora de proteger los datos mejorando así la percepción de seguridad de los consumidores y que las empresas logren incrementar sus ingresos.

Palabras Clave: Ciberseguridad, Comercio Electrónico, COVID-19, Pasarelas de pago, Vulnerabilidades.

Introducción

Debido a la pandemia de COVID-19 que se vive desde el año 2020 y la imposibilidad de ir a sitios públicos con aglomeración de gente, los comercios a nivel mundial implementaron y reforzaron sus canales de compra por medio de Internet, esto adicionado a una campaña publicitaria importante logrando que los hábitos regulares del consumidor cambiarán por completo incrementando las compras por medio de las diferentes plataformas de comercio electrónico o e-commerce (Medina, 2021), esto en teoría es mucho más fácil para el consumidor final a la hora de realizar una compra pero también implica una serie de riesgos, los cuales en su gran mayoría son los ataques cibernéticos que aumentaron a la par con el crecimiento de las compras en línea, por esto tanto el comercio como el consumidor está frente a la probabilidad de que ocurra una vulnerabilidad o amenaza cibernética que comprometa la integridad de sus datos.

En los últimos años, las empresas están utilizando las tecnologías de la información y la comunicación como herramientas en la prestación de servicios, gestión de dinero, compra y venta de productos y servicios, además de estar cambiando el modo en el que las empresas y personas se relacionan entre sí transformando patrones de conducta que anteriormente no se veían de forma frecuente; (Barrera Barrera, Bravo García, et al.2014) estos cambios en la sociedad y la economía de forma vertiginosa han hecho que se busquen nuevas oportunidades para facilitar y expandir el comercio en tiempos de pandemia.

No obstante, se debe considerar que el uso de tecnologías emergentes para el desarrollo de comercio en línea implica una serie de riesgos que comprometen no solo su propia información y la información que depositan los consumidores, sino que trasciende a mayores repercusiones

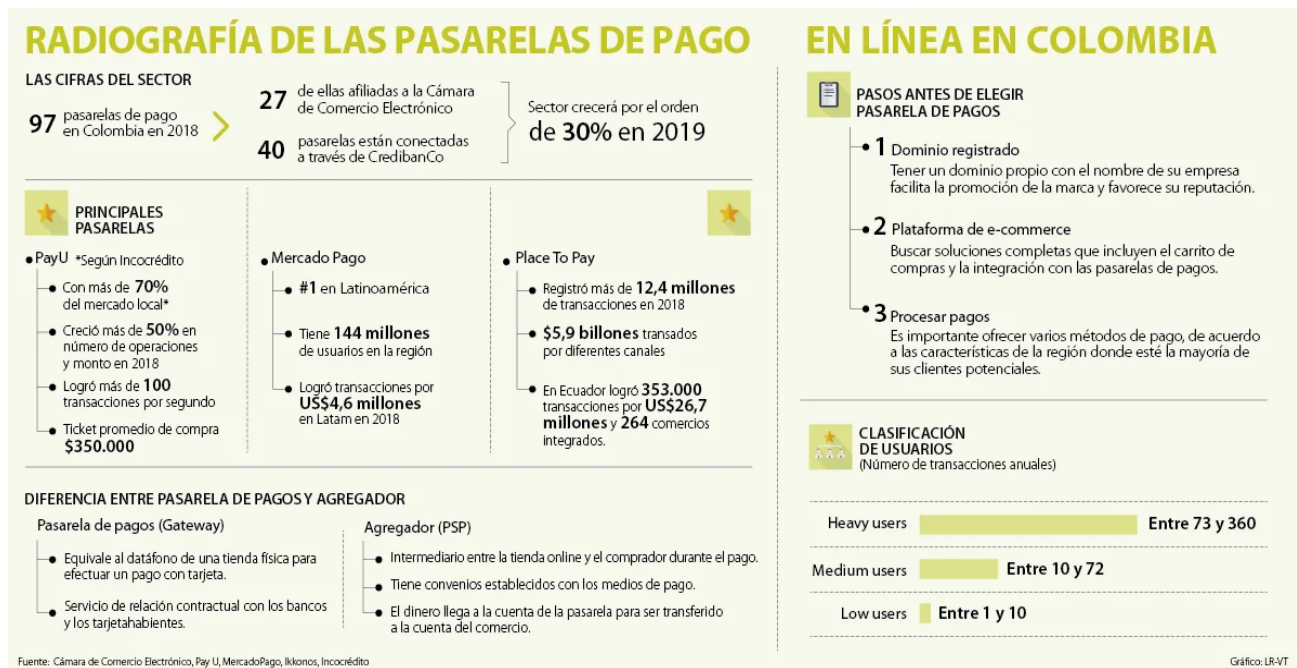
tanto a nivel económico, pérdida de activos financieros, pérdida de confianza y reputación e incluso tener consecuencias de ámbito legal por fuga de información privilegiada y data sensible. (Ceballos Lopez et al., 2019) por lo que es necesario conocer las vulnerabilidades y riesgos que conlleva el uso de pasarelas de pago y comercio en línea e identificar las mejores prácticas en Seguridad de la Información para fortalecer la cultura de concienciación, ciberseguridad y confianza digital entre empresas y consumidores.

El desarrollo del comercio electrónico en América Latina, especialmente en Colombia, han logrado una representación importante en la economía del país; con tendencia al crecimiento y posicionamiento dentro del mercado; gracias a la implementación de las pasarelas de pago electrónico que día a día evolucionan mejorando sus características de servicio y siendo así aprovechadas por el sector comercial y financiero para incrementar su competitividad y la confianza de los consumidores para que sea cada vez más sencillo y accesible adquirir servicios y productos a través de Internet (Ceballos Lopez et al., 2019).

Para el caso colombiano específicamente, de acuerdo a los datos de la Cámara Colombiana de Comercio Electrónico (CCCE), las pasarelas de pago en línea ya alcanzan a 97 a fines de 2018, siendo esto un crecimiento de 53,9% en comparación a fechas anteriores. De estas plataformas, 27 están afiliadas a la CCCE y las demás funcionan de forma independiente y 40 de ellas están conectadas a la red de Credibanco (Venegas Loaiza, 2019).

Figura 1.

Radiografía de las pasarelas de pago en línea en Colombia.



Nota. La gráfica corresponde a la situación de las pasarelas de pago en línea en Colombia a 2018. [Grafico], 2019, Diario La Republica (<https://www.larepublica.co/internet-economy/el-numero-de-pasarelas-de-pago-en-linea-en-colombia-ha-crecido-539-2828821>).

Para el desarrollo de este documento se describe en el capítulo 1 las generalidades del comercio electrónico; en el capítulo 2 las generalidades de las pasarelas de pago, en el capítulo 3 se detalla el marco regulatorio aplicable a Colombia para la implementación de comercio en línea; en el capítulo 4 se describen las principales vulnerabilidades que pueden afectar a los usuarios de comercio electrónico; en el capítulo 5 se analizan los resultados de la encuesta realizada por los autores del documento en la que se buscó conocer los hábitos de comportamiento y alcance actual del comercio en línea y en el capítulo 6, se formulan una serie de recomendaciones para los usuarios a la hora de utilizar pasarelas de pago.

Planteamiento del problema.

Para nadie es un secreto que todo lo que se encuentra en línea está al alcance de los ciberdelincuentes, por lo tanto los usuarios finales de los servicios de e-commerce no son la excepción; ante el auge y crecimiento exponencial en muchos de los sectores que intervienen y debido a las restricciones en establecimientos físicos por la crisis de la pandemia COVID-19 se generó un crecimiento en la implementación y uso de las plataformas de comercio electrónico y pasarelas de pago de las cuales hay susceptibilidad a los riesgos ya que no se tiene mayor conocimiento de su operación y alcance.

El desarrollo de herramientas por parte del sector financiero destacan de forma significativa, sin embargo, estas se encuentran orientadas principalmente al sector bancario por lo que es poco o nulo el conocimiento de las pasarelas de pago al momento de realizar transacciones comerciales; durante la contingencia generada por el aislamiento preventivo obligatorio en Colombia, el uso de canales y medios de pago digitales han jugado un rol fundamental para la economía, siendo métodos eficaces y eficientes para las compras en línea y siendo una alternativa atractiva para los consumidores; tanto estas herramientas como las compras en físico cumplen un rol determinado complementando entre sí y brindando estabilidad y solidez al sistema financiero.

Sin embargo, no solo los servicios e-commerce se encuentran expuestos a riesgos sino que se incluyen a las empresas que prestan este servicio y a los usuarios finales o los compradores que se ven expuestos a riesgos que en muchos casos se pueden presentar por intromisión de terceros, falta de planeación y recursos por parte de las empresas, preferencia a comprar físicamente en los

comercios por miedo o desconocimiento de los canales virtuales de compra y la baja cultura en ciberseguridad de los usuarios en línea desconocen o ignoran pero que puede causar un impacto en el proceso de compra en línea y en la percepción de confianza entre compradores y empresas afectando la reputación y credibilidad en estos procesos; por lo tanto es necesario realizar y resolver la siguiente pregunta: ¿Cómo lograr que el comprador en línea entienda y prevenga los riesgos de ataques informáticos a la hora de usar servicios e-commerce, concretamente pasarelas de pago dado el impacto generado a la hora de robar datos.

Objetivo General

Identificar y describir los ataques informáticos dirigidos a los usuarios finales que están motivados o que realizan regularmente compras en línea y cómo prevenirlos usando las mejores prácticas de la industria garantizando la protección de datos desde la primera cadena del eslabón (consumidor) de la seguridad de la información..

Objetivos Específicos

- Informar las principales vulnerabilidades a las que pueden estar expuestos los usuarios finales de los servicios de e-commerce y que pueden llegar a generar robo de datos personales y de tarjeta.
- Exponer los marcos de seguridad que debe cumplir un comercio con el fin de garantizar la seguridad de los datos que el usuario final dispone en las plataformas en línea.

- Analizar los hábitos de comportamiento e implementación de pasarelas de pago a raíz de la Pandemia COVID-19.
- Formular un plan de recomendaciones generales dirigidas al usuario final de servicios de e-commerce para la protección de sus datos ante ataques informáticos.

Metodología.

Para lograr el cumplimiento de los objetivos planteados en el presente proyecto dar cumplimiento a los objetivos planteados en el presente proyecto de investigación, se realiza una exploración teórica a partir de otros trabajos relacionados con el tema y que permitieran ampliar los conceptos y perspectiva actual acerca del funcionamiento de las pasarelas de pago y su relación con la ciberseguridad y la Seguridad de la Información teniendo en cuenta el avance de estos campos en Colombia; igualmente ampliando el conocimiento sobre comercio electrónico, haciendo énfasis en los riesgos cibernéticos y la cultura en Seguridad de la Información. Se recopiló documentación de entidades gubernamentales y financieras que ayudarán en la construcción del documento y permitieran el desarrollo la investigación mixta del tema (desarrollando enfoque cualitativo y cuantitativo).

En el estudio de Cortés Cortés et al., 2004; el enfoque de investigación mixto utiliza técnicas de investigación cualitativa y cuantitativa de forma separada para alcanzar los objetivos y lograr su medición y alcance, en el enfoque cuantitativo se realizan encuestas acordes al tema de investigación y que puedan ayudar a demostrar de forma medible los resultados de investigación utilizando la estadística para realizar el relevamiento de los datos y su correspondiente análisis

posterior y para el enfoque cualitativo, por medio del análisis de los marcos de referencia, investigaciones previas y antecedentes del tema se propone indicar la situación actual del uso de pasarelas de pago en Colombia, su enfoque y relación con la Seguridad de la Información, sus vulnerabilidades y desarrollo que se pueda tener a futuro.

El alcance que se desea tener con la investigación es de carácter descriptivo; ya que con el análisis de la situación del comercio electrónico a raíz del COVID-19 y el incremento del uso de pasarelas de pago, se pretende informar los riesgos y vulnerabilidades inherentes a estos medios y como ha sido el desarrollo o falta de él en materia de regulación y ciberseguridad para posteriormente brindar las recomendaciones necesarias para el uso e implementación de estos.

Justificación

El propósito del presente documento radica en dar a conocer la importancia del uso de las pasarelas de pago en el sector comercial y como están influyendo en los nuevos hábitos de consumo a raíz de la pandemia COVID-19, teniendo en cuenta el crecimiento del comercio en línea en los últimos meses y su impacto en la digitalización de procesos comerciales es vital conocer las diferentes alternativas en cuanto al uso y aprovechamiento de la tecnología ajustándose a las necesidades de cada empresa y que faciliten la experiencia de los consumidores al momento de adquirir servicios o bienes de una forma rápida y sencilla siendo una oportunidad de innovación y competitividad en el mercado.

Con este preámbulo, las empresas colombianas se han decantado por incursionar en el comercio electrónico para reactivarse económicamente y como una alternativa novedosa para posicionarse

en el mercado, no obstante, a medida que avanza la tecnología, este cambio se está dando de forma más dinámica y vertiginosa en la que se involucran nuevos actores y modelos de negocio que buscan mantenerse en un motor de crecimiento que no se daba en años anteriores. Sin embargo, no todas las empresas ni consumidores se encuentran en condiciones de adaptarse a este nuevo cambio generando una brecha significativa a medida que avanza esta transformación digital.

También es importante tener en cuenta que a nivel nacional hasta el año 2020 no se contaba con una reglamentación sólida para la regulación y la puesta en marcha de las pasarelas de pago, algo bastante preocupante dado que ninguna de ellas estaba obligada a cumplir con la implementación de mejores prácticas o estándares internacionales de aseguramiento de los datos y hasta diciembre del año 2020, debido al marco de la pandemia COVID-19, al crecimiento exponencial de las transacciones en línea y la imposibilidad de adquirir artículos de la manera como la gran mayoría de las personas lo hacían antes (presencialmente), por lo que se promulga por parte de la Presidencia de la República el Decreto 1692 de 2020 *“Por medio del cual se modifica el Decreto 2555 de 2010 en lo relacionado con los sistemas de pago de bajo valor”* (Ministerio de Hacienda y Crédito Público) el cual realiza una serie de recomendaciones a la Superintendencia Financiera con el fin de iniciar un ejercicio exhaustivo de controlar y vigilar todos los aspectos anteriormente mencionados, esto fundamentando como pilar principal de todos los organismos que se dedican a este tipo de actividades que propendan por la Seguridad de la Información, lo que conlleva a que el ámbito de pasarelas de pago en Colombia se ofrezca un amplio portafolio de soluciones las cuales se van a estar desarrollando y explicando a detalle en este proyecto.

También se debe propender por el fortalecimiento de la cultura de concienciación en ciberseguridad; entendiendo la operación, responsabilidad y alcance de estos procesos comerciales; no solo orientado al sector bancario sino que en un futuro no muy lejano se promueva la creación de una política general enfocada a pasarelas de pago en la que se tenga como principal actor al consumidor final y que reúna la normativa y regulación necesaria para aprovechar y afrontar los retos asociadas a las dinámicas del cambio tecnológico consecuentes al COVID-19.

Capítulo I.

Comercio electrónico en Colombia.

El comercio electrónico (Electronic Commerce, o e-Commerce) se puede definir como las actividades de adquisición de bienes y servicios empleando herramientas electrónicas y web facilitando la automatización en los procesos de compra, minimizando los costos y tiempos de operación y mejorando la experiencia en la interacción entre usuarios y empresas. En el año 1999, Colombia fue país pionero en Latinoamérica en definir los lineamientos del comercio electrónico e involucrar sus el funcionamiento de transacciones comerciales a través de canales electrónicos, esto por medio de la Ley 527 de 1999 *"Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones"* (Congreso de Colombia, 1999). Con esta ley se inicia la reglamentación del acceso y uso de mensajes de datos como

medio válido para actividades comerciales y define los atributos legales y jurídicos de la firma digital.

Para el caso colombiano, en el comercio en línea entre los sistemas de pago más comunes se encuentran las bancas móviles, portal transaccional bancario web, datafonos y tarjetas con tecnología contactless, billeteras electrónicas, pasarelas de pago, PSE (pagos seguros electrónicos). Adicionalmente, el comercio electrónico, basándose en las mejoras tecnológicas de las Tecnologías de la Información y la Comunicación ha facilitado los procesos comerciales reduciendo los costos transaccionales, brindando información a los usuarios, aumentando el número de bienes y servicios y la participación en el mercado entre otros factores conllevando a ganancias eficientes y siendo el motor potencial de crecimiento económico (Comisión de Regulación de Comunicaciones, 2017).

1.1 Tipos de comercio electrónico.

Business-to-Business (B2B) Negocio a Negocio: Este tipo de operaciones se produce entre dos empresas con presencia en Internet donde no intervienen los consumidores finales. (Villalba, 2021). No intervienen los clientes regulares, en este tipo de comercio los vendedores buscan compradores, los compradores buscan proveedores o bien los intermediarios concretan acuerdos comerciales entre vendedores y compradores.

Business to Consumer (B2C) Negocio a Cliente: Tipo de transacción entre una empresa y un consumidor o persona particular en el que el consumidor adquiere un producto o servicio de interés por medio de la empresa; es el tipo más común de transacción comercial siendo uno de los

canales más fuertes a nivel de ventas y de optimización de mercadeo, siendo la empresa quien se encarga de los procesos de compra y distribución además de habilitar los canales de comunicación hacia los clientes y proporcionar la información de forma segura y en tiempo real. Un ejemplo de este tipo de comercio es Amazon.

Business to Employee (B2E) Negocio a Empleado: Se trata de todo lo que una empresa puede proporcionar, en materia de bienes y servicios, a sus empleados directamente desde su tienda online, de su portal de Internet o de la Intranet empresarial. Por lo general los productos o servicios tendrán precios especiales con el objetivo de incentivar a los colaboradores y fortalecer la relación con la empresa; además, este tipo de comercio electrónico se realiza en una sesión con control de acceso exclusivo para cada compañía.

Consumer to Business (C2B) Cliente a Negocio: Aunque no es un modelo de negocio tan común, este tipo de transacción se da entre una persona que ofrece sus servicios o productos a empresas u organizaciones, siendo el consumidor quien fija los términos de venta en su mayoría de servicios.

Consumer to Consumer (C2C) Cliente a Cliente: Este modelo de negocio se da entre consumidores y usuarios finales, sin que intervenga ninguna empresa de manera directa pero si en modalidad de mediadores y garantes de la compra y venta. Para ello se emplean sitios web que proveen una plataforma de intercambio desde donde los consumidores realizan sus transacciones económicas, si la operación se concreta el sitio recibe una comisión por la venta realizada. Algunos ejemplos de esta modalidad son Ebay y Mercadolibre.

Government to Consumer (G2C) Gobierno a Cliente: Es cuando un gobierno a través de la digitalización de los procesos y trámites que correspondan permite que los ciudadanos realicen sus trámites y los paguen a través de un portal. Su gran ventaja es el ahorro del tiempo y la seguridad que puede brindar el respaldo electrónico, y es muy común para el pago de impuestos. Este tipo de comercio no solo involucra el pago de una tasa, impuesto o gravamen sino también para consultas de trámites en general y acceso a información específica de interés del ciudadano.

Capítulo II.

Pasarelas de pago.

Los sistemas de pagos digitales son la herramienta tecnológica encargada de habilitar y procesar los pagos digitales entre empresas y ciudadanos que hacen uso del comercio electrónico, siendo equivalente al datáfono de una tienda física para efectuar pagos con tarjeta de crédito o débito. De acuerdo con el balance de la CCCE (Cámara Colombiana de Comercio Electronico) con corte a 2018, ya hay 97 pasarelas de pago que operan en todo el país, una cifra que se traduce en un crecimiento de 53,9% si se tiene en cuenta que para 2017 se reportaron 63 plataformas en operación (Bohórquez Guevara, 2019). Estas plataformas logran beneficiar tanto a los comercios online como a los internautas que buscan mayor seguridad, accesibilidad, variedad, rapidez en sus compras y una variedad de medios de pago que no solo se limitan al efectivo y a la tarjeta de crédito.

Las pasarelas de pago funcionan como intermediario entre la tienda en línea y la cuenta bancaria del vendedor; traslada la información suministrada por el comprador a los administradores de las

redes de pago y transfieren al comprador la información relacionada con el resultado de la verificación realizada por las redes procesadoras de pago. Para las pasarelas de pago hay dos modalidades de funcionamiento: Agregador y Gateway; para el modelo agregador el dinero llega de forma directa a la cuenta bancaria de la plataforma de pago y de allí se transfiere a la cuenta del vendedor. En el modelo Gateway, el dinero llega directamente a la cuenta del comercio que vende el producto y depende de cada comercio implementar cualquiera de los modelos que se adapte mejor a sus necesidades (Comisión de Regulación de Comunicaciones, 2017).

Al momento de elegir una pasarela de pagos se debe tener en cuenta una serie de factores que garanticen la confianza y tranquilidad a la hora de realizar transacciones comerciales, se debe evaluar los costos de implementación, certificaciones en seguridad, atención al usuario, soporte en línea, franquicias, métodos de pago y flexibilidad entre otros. Para este propósito, de acuerdo a la entrevista brindada a (Portafolio.co, 2021) por parte de Jairo Camargo, gerente de Tu Pago, explica los principales factores que deben garantizarse a la hora de elegir una pasarela de pagos:

- **Certificada:** Tras el decreto 1692 de 2020 se busca regular la certificación de los sistemas de pago de bajo valor, además la pasarela de pago debe contar con certificación PCI DSS (Payment Card Industry Data Security Standard); la cual es otorgada cuando se adoptan las recomendaciones brindadas por el PCI Security Standards Council para el uso y manejo de la información de tarjetas tanto débito como crédito.
- **Transversal:** Se debe contar con el servicio para venta presente (uso de datáfono móvil o fijo) y no presente (comercio por internet).

- Incluyente: Se debe ofrecer diversas formas de pago como tarjeta de crédito, tarjeta débito, efectivo, PSE y otras plataformas para la población no bancarizada.
- Segura: Esto es con el objetivo de blindar al consumidor de ataques por fraude, rechazo, hurto, fuga de información u otros que puedan comprometer la transacción comercial.
- Adaptable: Cuando un comercio no cuente con página web, la pasarela puede brindar un enlace de cobro para remitir al consumidor y que pueda realizar la transacción desde cualquier dispositivo con el método de pago que elija. En cambio, cuando el comercio cuenta con portal web se provee un plugin o complemento de fácil integración a la pasarela de pago.

En Colombia, en la actualidad hay varias empresas que prestan este servicio, con amplia trayectoria y mercado, entre las más populares están PayU, Wompi, MercadoPago, PayPal, EPayco, PlacetoPay entre otras.

Capítulo III.

Marco normativo y regulatorio.

Para hablar de un marco de referencias en el ámbito de la ciberseguridad enfocada específicamente hacia el comercio en línea es necesario conocer los estándares y leyes aplicables a Colombia que repercuten en los consumidores y empresas, una de ellas es la Ley 1480 de 2011 o Ley de Protección al consumidor *"Por medio de la cual se expide el estatuto del consumidor y se dictan otras disposiciones"* (Congreso de Colombia, 2011), esta ley tiene como objeto proteger, promover y amparar al consumidor y sus intereses económicos frente a riesgos para su

salud y seguridad, garantizar información adecuada acorde a los términos de ley entre otras siendo aplicable a todo el territorio nacional, se dictaminan los derechos y deberes del consumidor brindando las garantías legales y los mecanismos ante los cuales pueda interponerse una reclamación.

Respecto a protección de datos personales, se promulga la Ley Estatutaria 1266 de 2008 o Habeas Data *“Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones”* (Congreso de Colombia, 2008) que regula el manejo de información de bases de datos personales, principalmente las de tipo financiero, crediticio, servicios y de terceros estableciendo que los datos de carácter personal pueden ser de tipo privado, semi privado y público. Otra de las leyes que rigen en Colombia es la Ley 1581 de 2012 *“Por la cual se dictan disposiciones generales para la protección de datos personales”* (Congreso de Colombia, 2012) , la cual define las categorías especiales de datos personales, ámbito de aplicación, derechos y deberes de los titulares entre otras disposiciones, cabe mencionar que si bien estas leyes son aplicables en Colombia y buscan garantizar un entorno seguro para la población, en la mayoría de casos se desconoce su contexto, su aplicación y vigencia. Es por esto, que se debe impulsar una socialización de estas normas y cómo deben ir alineadas a los procesos comerciales en línea y que no solo sea la empresa quien conozca las leyes sino el consumidor.

Con el creciente uso de las Tecnologías de la Información y las Comunicaciones (TIC); el incremento de conexiones a Internet y la masificación de servicios y actividades en línea hacen

evidente un aumento sustancial en el uso de canales virtuales para el desarrollo de actividades socioeconómicas que, anteriormente se daban en forma presencial. Sin embargo, este aumento de participación digital y más en el comercio electrónico acarrea riesgos de seguridad digital tanto para empresas como consumidores que, de no ser identificados y gestionados de forma adecuada pueden derivar en ataques cibernéticos con una alta repercusión económica y/o social para el país (Organización de los Estados Americanos et al., 2017). Por esto, una de las primeras políticas en materia de seguridad digital para Colombia es la Política Nacional de Seguridad Digital CONPES 3854 de 2016, liderada por los Ministerios de Defensa Nacional y de Tecnologías de la Información y las Comunicaciones; esta política busca articular a los entes gubernamentales, organizaciones públicas y privadas, Fuerza Pública, propietarios y operadores de las infraestructuras críticas cibernéticas nacionales para que hagan un uso eficaz y responsable de los entornos digitales y puedan a su vez identificar, gestionar y mitigar los riesgos de seguridad digital.

Ya para el 2020, se expide la Política Nacional de Comercio Electronico (CONPES 4012) , liderada por el Departamento Nacional de Planeación (DNP), Ministerio de Comercio, Industria y Turismo y el Ministerio de Tecnologías de la Información y las Comunicaciones y cuyo principal objetivo es impulsar el comercio electrónico en las empresas y en la población para incrementar la generación de valor social y económico del país; y para llegar a este objetivo se busca generar las capacidades técnicas necesarias para el uso, apropiación e implementación del comercio en línea a nivel de empresas y posteriormente, en la sociedad actualizando el marco regulatorio que ayude a impulsar el comercio electrónico. De acuerdo a lo planteado en el documento CONPES

se tiene trazado un horizonte de 5 años a partir de 2021 y hasta el 2025. (Departamento Nacional de Planeación et al., 2020).

Para el INCIBE (2015) los usuarios de los comercios electrónicos están comprometidos y expuestos a una serie de amenazas que pueden llegar de una amplia gama de vectores de ataque debido al contexto globalizado en el que nos encontramos en este punto de la historia, amenazas o ataques que comprometen tanto el desarrollo íntegro de la operación del comercio electrónico y que también genera desconfianza en los usuarios a la hora de usarlos, esto teniendo en cuenta que este tipo de transacciones en los años posteriores van a seguir creciendo de una manera agigantada y por lo tanto usuarios finales, empresas y demás actores deban adaptarse y estar en una evolución constante.

La velocidad y la cantidad con la que se ejecutan las transacciones hoy en día por estos canales hace que los ciberdelincuentes se sientan atraídos por la información que se encuentra transmitida con el único objetivo de obtener un beneficio económico apoderándose de la información confidencial de los clientes de un comercio electrónico esto con el fin de poder vender la información hurtada o sacar provecho de esta y usarla para configurar otro tipo de ataques como el de dañar la imagen de una empresa por lo tanto las empresas u organizaciones no pueden pasar por alto las amenazas que están dirigidas sus clientes porque su base para operar es la confianza que estos les brindan a la hora de realizar un pago o una compra a través de los canales que propone para dicha actividad.

De acuerdo a lo mencionado por McKee (2021) el COVID-19 ha jugado un rol bastante importante como impulsor de la gran mayoría de cambios que se han realizado en el último año

en cuanto a las transacciones en línea y la conducta de compra de los usuarios de los comercios habituales haciendo que las cifras relacionadas a este tipo de comercio crezcan alrededor de un 23% en ventas en billones de dólares de igual manera durante la pandemia el 72% de los clientes migraron sus compras de la presencialidad a las compras en línea lo que habla y expone un cambio significativo en los hábitos de compra que hasta el momento se han mantenido de esta manera, pero no todos los que adoptaron el modelo de comprar en línea se vieron satisfechos a la hora de realizar su compra de manera ágil y efectiva por el gran obstáculo que corresponde los fraudes y los ataque cibernéticos de los que fueron víctimas debido a una combinación de factores como lo son la nula experiencia a la hora de realizar un pago electrónico, la experiencia negativa del usuario y claro está debido a la pandemia la crisis económica afectó a muchas personas y empresas haciendo que cada cantidad de dinero que se gasten por más pequeña que sea vuelva más importante y valiosa que nunca.

En el siguiente gráfico se puede observar el porcentaje de cada de las iniciativas de los comercios para mejorar su entorno de pagos digitales de acuerdo a los resultados obtenidos en el estudio.

Figura 2.

Enfoque de los comercios e iniciativas presentadas para mejorar el entorno de pagos digitales



Las empresas no solo deben enfocarse en las ciberamenazas que generan pérdidas a nivel económico (INCIBE) si no también en las que causan impacto a la imagen corporativa del comercio en este caso, y esa es la base de un comercio la confianza que tienen su clientes a la hora de ejecutar una compra por cualquiera de los canales que se implementan, por este motivo es necesario e indispensable tener una visión global de los ataques a los que se encuentran expuestos sea directa o indirectamente y al tener claro estos vectores de ataque pueden abordarlos para disminuir el riesgo ante lo que conoce como el eslabón más débil de la cadena el cual es el usuario final.

El desconocimiento de las personas ante los actores involucrado en las compras en línea como son pasarelas de pago, comercios, adquirentes y bancos hace que estos se piensen dos veces a la hora de realizar una compra porque no saben a quien le entregan sus datos y donde van a reposar luego de la compra por lo tanto es fundamental que los usuarios finales conozcan los diferentes actores y su manera operar al conocerla les brinda un plus de confianza del funcionamiento de la compra y adicionalmente del destino final de sus datos.

Capítulo IV

Vulnerabilidades asociadas al comercio en línea.

El uso malicioso de las tecnologías de la información y las comunicaciones, junto con la globalización vertiginosa presente en la sociedad enfrenta al consumidor de servicios en línea a los riesgos cibernéticos y vulnerabilidades derivadas del uso de estos servicios; estas vulnerabilidades pueden presentarse en el mismo inicio de compra o ya en el desarrollo de esta y puede generarse de forma intencional, deliberada o maliciosa por lo general de forma involuntaria: por un error en la pasarela de pago, errores de conexión a Internet, desconocimiento de algún proceso o falta de experiencia y en una menor medida, por falta de sentido común en el consumidor resultando en la pérdida de confidencialidad, integridad y disponibilidad de datos de parte de ambos actores (Organización de los Estados Americanos & Asobancaria, 2020).

Para los usuarios de los comercios electrónicos están comprometidos y expuestos a una serie de amenazas que pueden llegar de una amplia gama de vectores de ataque debido al contexto globalizado en el que nos encontramos en este punto de la historia, amenazas o ataques que

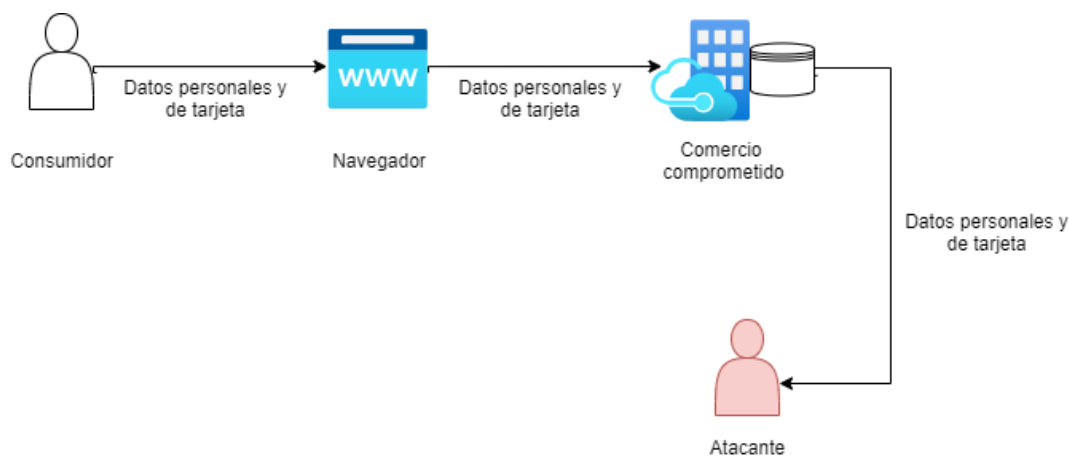
comprometen tanto el desarrollo íntegro de la operación del comercio electrónico y que también genera desconfianza en los usuarios.

De acuerdo con el informe de la Organización de Estados Americanos en conjunto con Asobancaria del 2019, durante el 2018 en Colombia se registraron 21.687 denuncias por delitos informáticos, siendo un incremento del 36% respecto al año anterior; de estos delitos, el hurto por medios informáticos fue el delito de mayor impacto con 12.014 denuncias y anualmente se van generando más delitos y mayor número de víctimas, según lo reporta el Centro Cibernético Policial (Organización de los Estados Americanos & Asobancaria, 2019). Por lo tanto en el presente trabajo vamos a exponer las vulnerabilidades conocidas y más comunes por donde los ciberdelincuentes toman partido con el único fin de robar los datos personales y de pago de los clientes. Algunas de las vulnerabilidades más comunes que pueden afectar a los consumidores de servicios de comercio en línea son:

- **Web Skimming:** Es un tipo de ataque que se configura cuando los cibercriminales proceden a cometer un robo de información de pago (datos de tarjeta y datos personales) de los usuarios luego de comprometer el e-commerce donde el cliente ha ingresado o está interesado en efectuar una compra.

Figura 3.

Ejemplo Web Skimming



- **Ingeniería Social:** Es un tipo de ataque que usan los ciberdelincuentes para engañar a los usuarios crédulos e inocentes con el fin de manipularlos con el único objetivo de obtener datos de estos y así poder sacar partido de estos en un futuro uso indebido o venta de los datos.

Figura 4.

Ejemplo Ingeniería Social



- **Spear phishing:** Son estafas que se dirigen o que se configuran vía correo electrónico hacia los usuarios donde la finalidad de esta es robar u obtener datos para fines delictivos.

Figura 5.

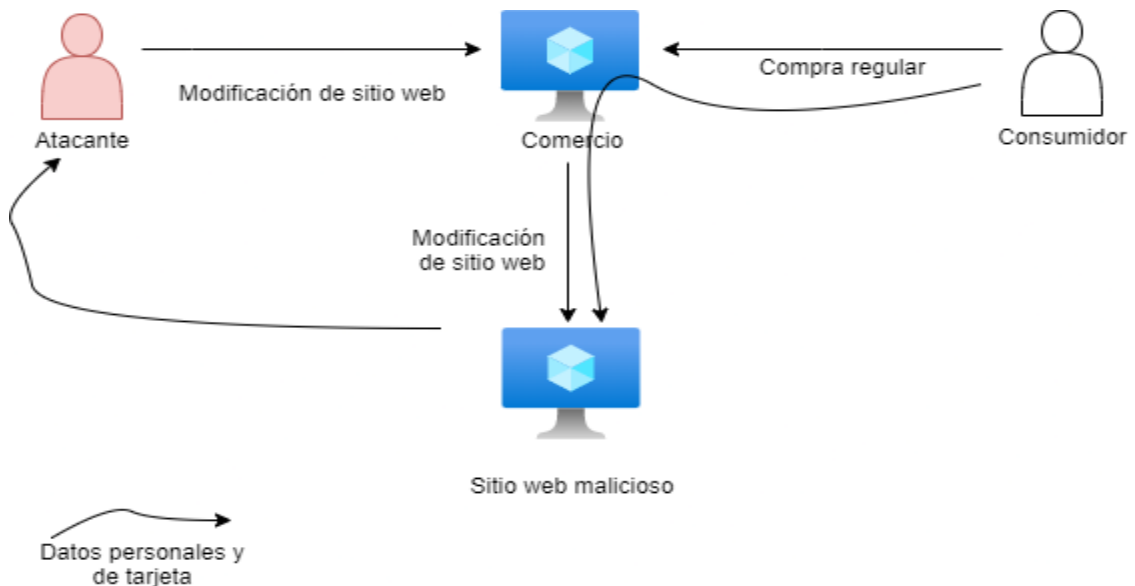
Ejemplo Spear Phishing



- **Defacement:** En este ataque se ven involucrados dos de los actores involucrados en una compra online la cual es la modificación o clonación de la página web de los comercios haciendo que su apariencia gráfica y su lógica cambien causando como consecuencia que los datos de los usuarios no sigan los flujos establecidos si no se dirijan a otro repositorio.

Figura 6.

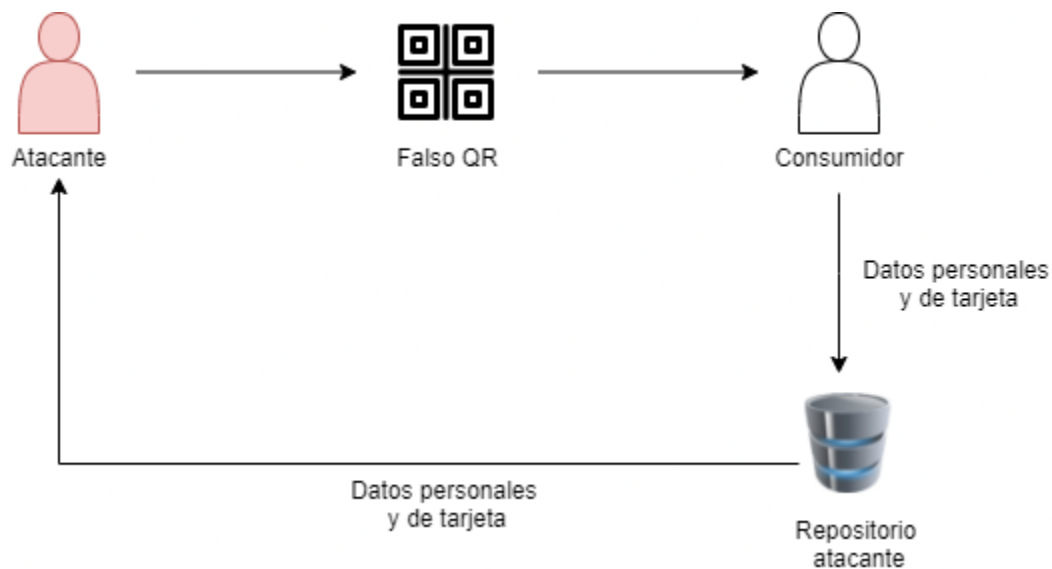
Ejemplo Defacement



- **Falsos QR:** Son códigos maliciosos donde aparte de muchas funciones maliciosas, la principal es dirigir a sitios web falsos o sitios que hacen la veces de phishing con el fin de que el usuario digite sus datos tanto personales como de pago dentro de un sitio web falso y esta información sea tomada por los ciberdelincuentes.

Figura 7.

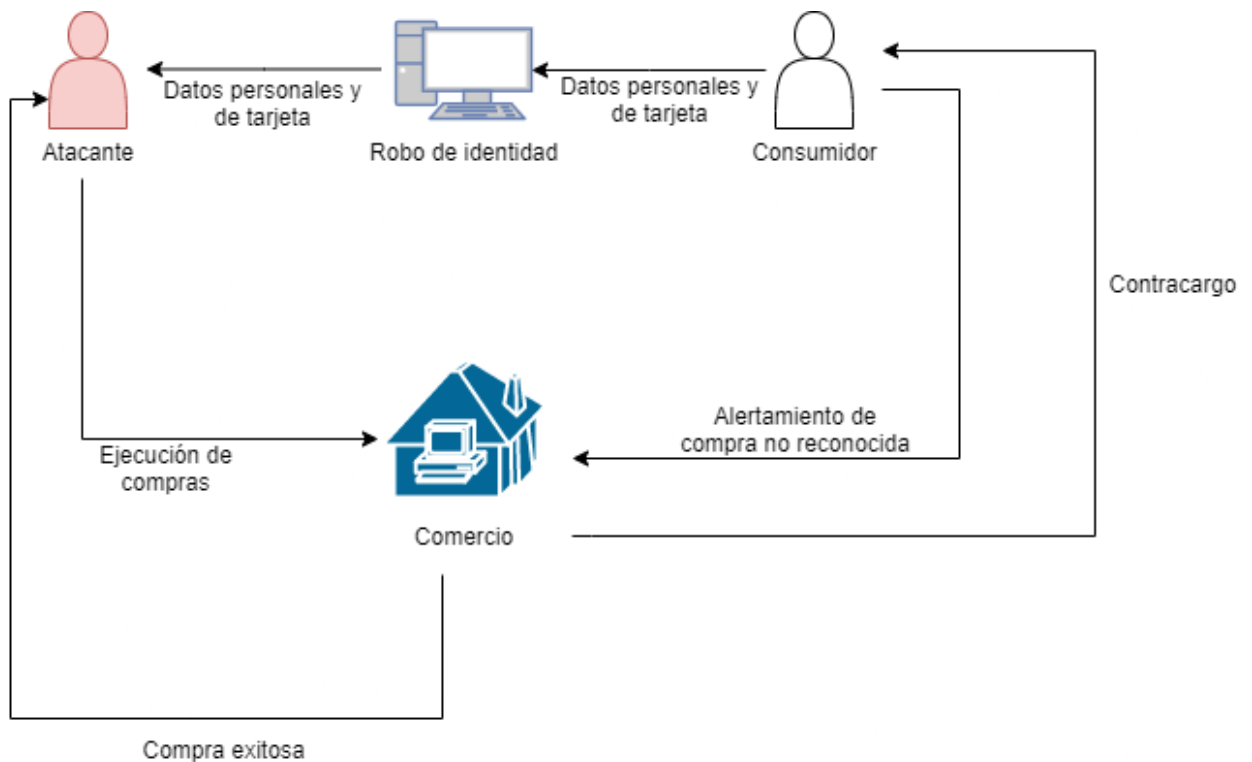
Ejemplo Falsos QR



- **Robo de identidad:** Este riesgo se configura una vez los ciberdelincuentes se hacen de los datos de la persona y los usan para realizar transacciones en los e-commerce afectando directamente al usuario final y de manera indirecta el comercio debido a que el usuario solicitara un contracargo y el comercio será el responsable de correr con el costo del ataque.

Figura 8.

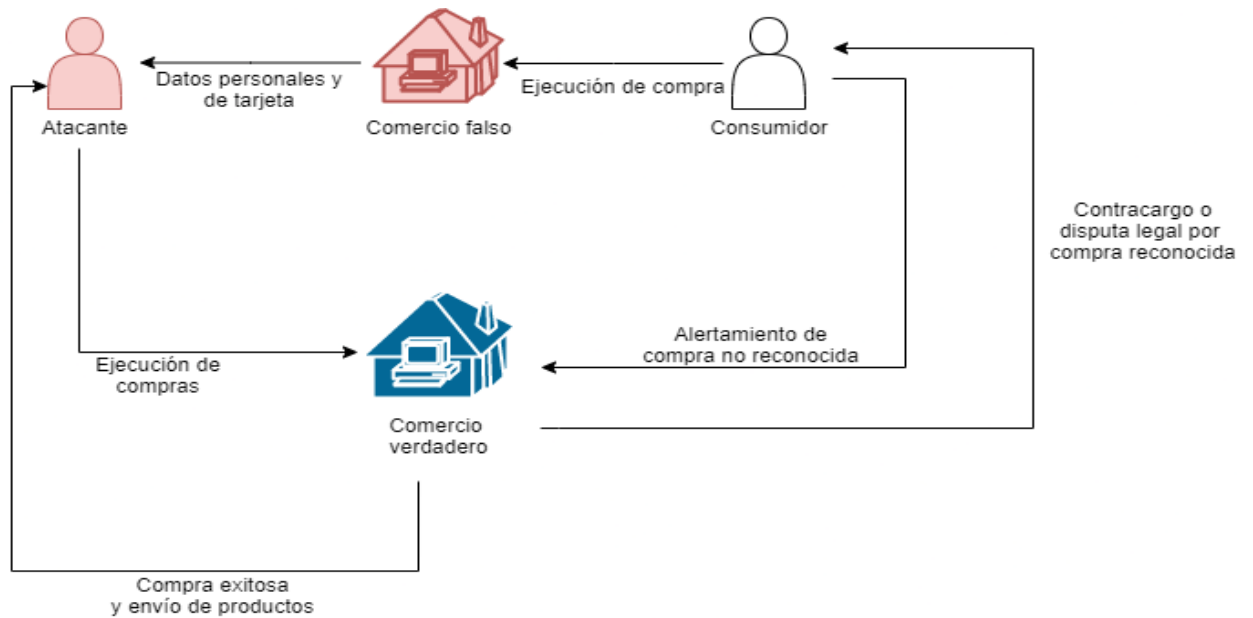
Ejemplo Robo de identidad



- **Fraude de triangulación:** En este tipo de fraude se ven igualmente involucrados dos de los actores principales en cuanto a compras por e-commerce se refiere, este se lleva a cabo cuando el ciberdelincuente mediante alguna de las vulnerabilidades hurta los datos de los clientes de los e-commerce y en tiempo real ejecuta la compra de manera legítima en el comercio haciendo que para ambas partes (comercio y usuario legítimo) esta transacción sea correcta y hecha de manera real pero los datos de envío fueron modificados y aparte hurtados los datos del comprador.

Figura 9.

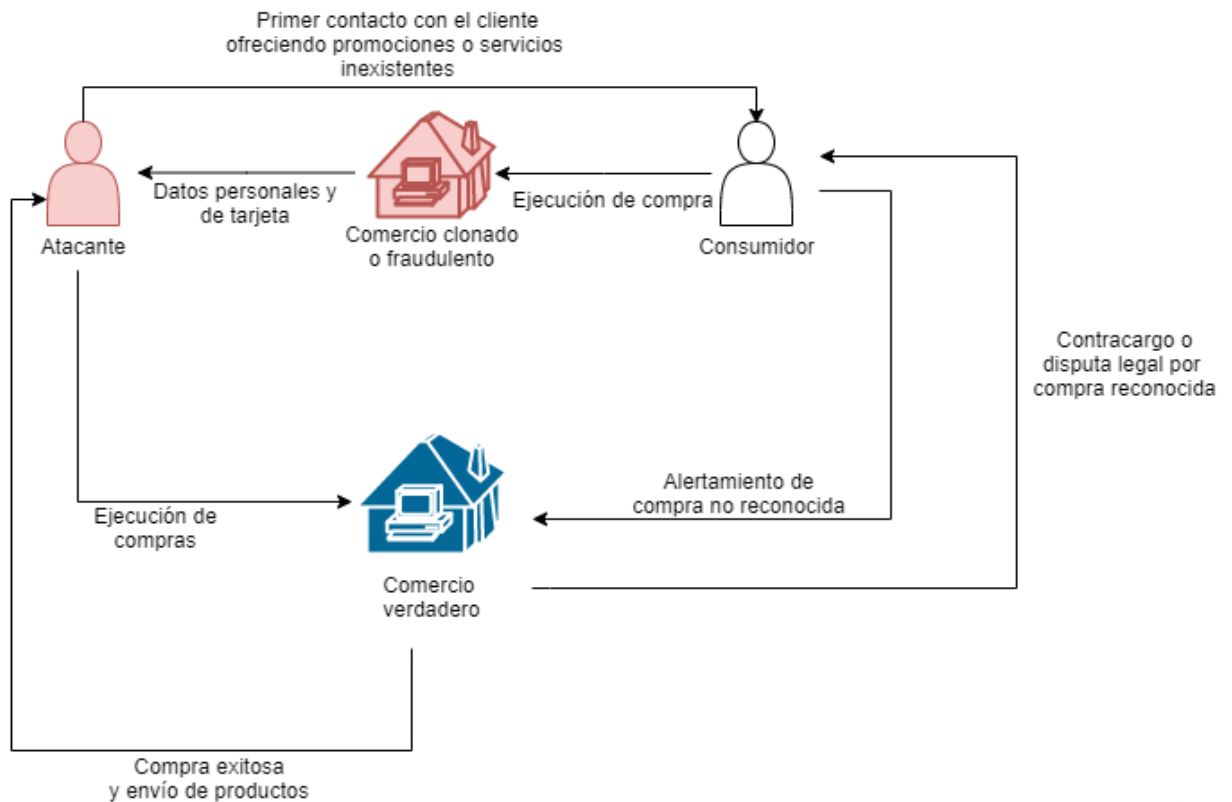
Ejemplo Fraude de triangulación



- **Fraude de identidad comercial:** Este tipo de ataque es bastante sofisticado y tiene a lugar con el ofrecimiento de descuentos, promociones o productos bastante llamativos para el comprador común pero son inexistentes se reciben los datos del cliente por medio de páginas clonadas o falsas haciendo que se entreguen datos de tarjeta y además dinero en ciertos casos por pagos de productos ficticios que realmente nunca serán entregados al comprador legítimo.

Figura 10.

Ejemplo Fraude de identidad comercial



- **Smishing:** Es un tipo de fraude que se ejecuta y se lleva a cabo en su totalidad por tecnologías de mensajería de usuario final (SMS, WhatsApp, Telegram) donde el ciberdelincuente envía mensajes a los usuarios haciéndose pasar por el comercio informando de promociones, regalos, descuentos y junto con ello un enlace que dirige a un sitio web falso donde se hurtan los datos de los usuarios.

Figura 11.

Ejemplo Smishing



- **Vishing:** Este fraude se ejecuta por medio de llamadas telefónicas haciendo prácticamente lo mismo que el phishing y el vishing, solicitando datos de tarjeta y personales por medio de voz de la misma manera ofreciendo ofertas tentadoras para los usuarios haciendo que sea complejo para ellos negarse a dar los datos salvo que ya conozca este modus operandi.

Figura 12.

Ejemplo Vishing



Describiendo estas vulnerabilidades cibernéticas, es necesario que se cuente con acciones eficaces y eficientes de remediación, capacitación y concienciación que minimicen estos eventos, ya que si bien hay campañas y formación en prevención antifraude estas se encuentran diseñadas y priorizadas para entidades bancarias y sus usuarios más no se abarca a los consumidores de servicios ecommerce en las pasarelas de pago. Las entidades financieras, por ejemplo, entre sus mecanismos de concienciación en materia de seguridad digital incluyen los banner en correos electrónicos emitidos por las entidades, capacitaciones y boletines los cuales han sido implementados por el 94 % de las entidades financieras del país (Organización de los Estados Americanos & Asobancaria, 2020)

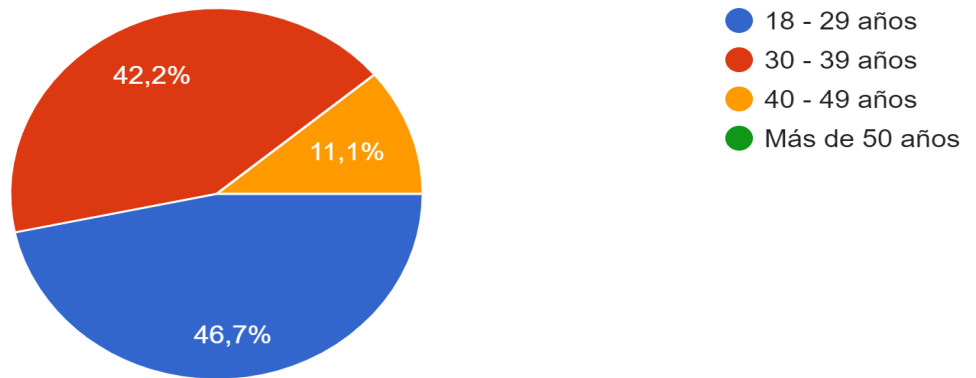
Capítulo V

Desarrollo Proyecto y Análisis de datos.

Para el desarrollo del proyecto se realizó una encuesta diseñada para personas mayores de edad, principalmente usuarios de servicios ecommerce, con la cual se pretende evaluar la situación actual de uso de pasarelas de pago y servicios ecommerce a raíz de la pandemia COVID-19 y si se tiene conocimiento básico de conceptos de ciberseguridad, vulnerabilidades y riesgos asociados a este sistema. A continuación, se exponen los resultados obtenidos para una muestra de 45 participantes:

Rango de edad.

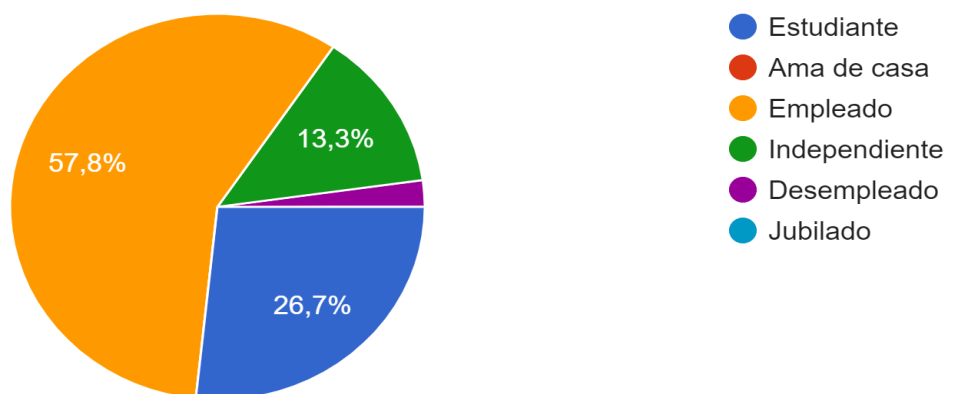
45 respuestas



De 45 participantes, el mayor porcentaje de personas se encuentran entre los 18 - 29 años y corresponde a 21 personas, seguido por 19 personas con rango de edad entre 30 - 39 años; y 5 personas se encuentran entre los 40 - 49 años. Con esto, se determina que es la población joven quien mayor alcance tiene al uso de los servicios de comercio electrónico y muy poca o nula participación de personas de mayor edad.

Indique su ocupación.

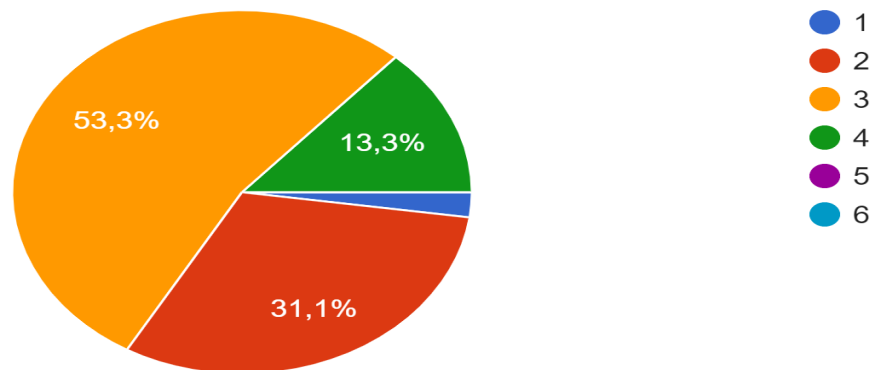
45 respuestas



De 45 participantes, el mayor porcentaje de personas encuestadas son empleados y corresponde a 26 personas, seguido por 12 personas estudiantes; 6 personas que se desempeñan en áreas independientes y 1 persona en desempleo.

Indique su estrato socioeconómico

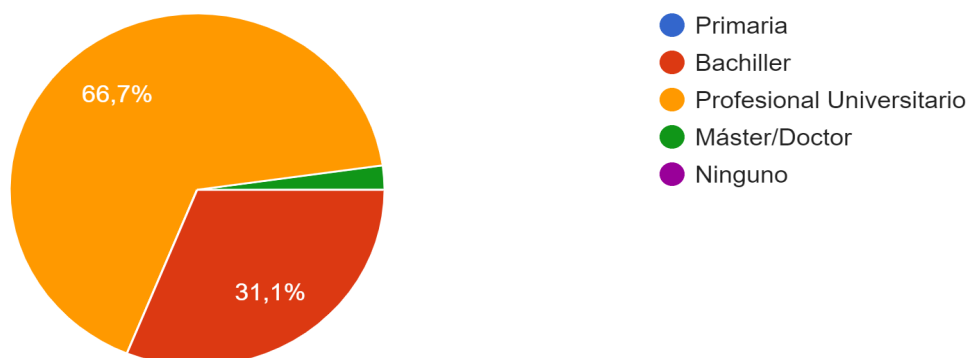
45 respuestas



De 45 participantes, el mayor porcentaje de personas encuestadas pertenecen al estrato 3 y corresponde a 24 personas, seguido por 14 personas de estrato socioeconómico 2; 6 personas de estrato socioeconómico 4 y 1 persona de estrato socioeconómico 1. Con esto, se observa que los estratos socioeconómicos promedio del país son quienes representan un mayor porcentaje de participación en el comercio.

Indique su nivel académico actual

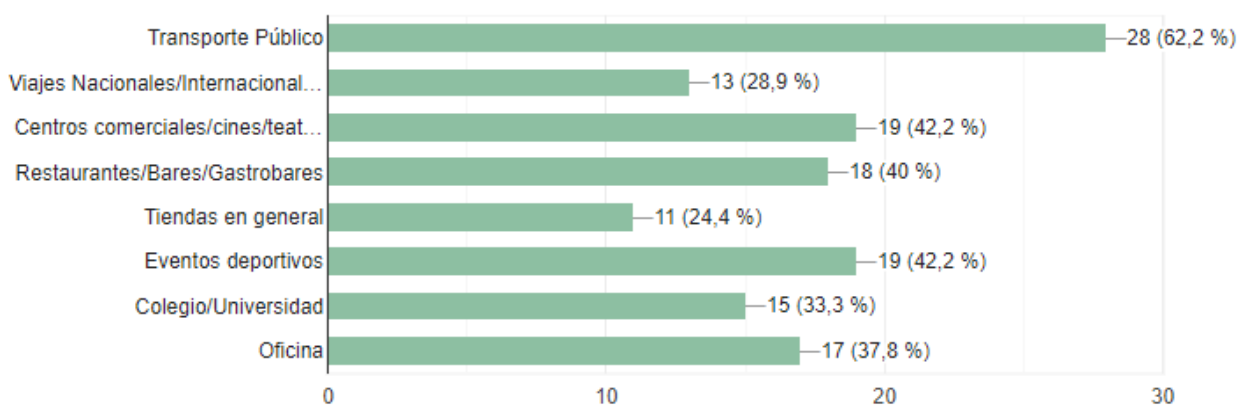
45 respuestas



De 45 participantes, el mayor porcentaje de personas son profesionales universitarios y corresponde a 30 personas, seguido por 14 personas bachilleres y 1 persona con estudio Máster/Doctor.

A raíz de la pandemia COVID-19, de estos sitios públicos, ¿Cuáles ha evitado o dejado de ir con la frecuencia con la que antes si lo hacía?

45 respuestas

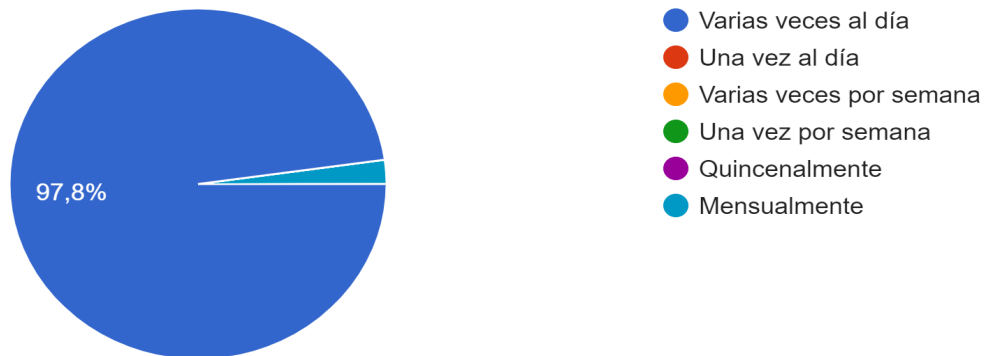


Se verifica que la mayoría de participantes a raíz del COVID-19 dejaron de utilizar el transporte público, seguido por la asistencia a centros comerciales y eventos deportivos y como menor

medida dejaron de ir a tiendas en general, cambiando así algunos hábitos de comportamiento que eran comunes en épocas pre pandemia.

¿Con qué frecuencia se conecta a Internet?

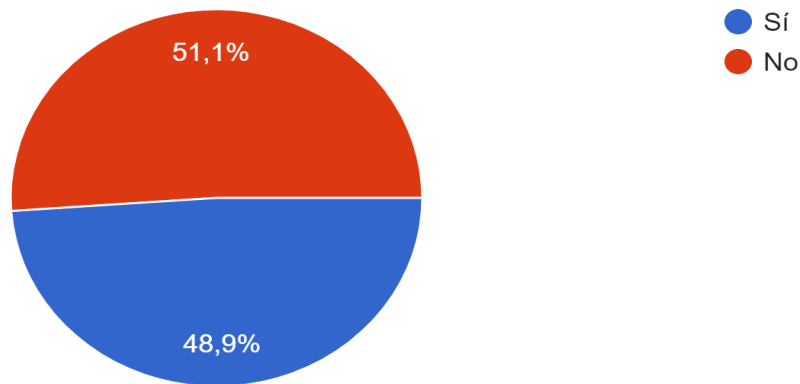
45 respuestas



De forma contundente, se observa que los participantes a la hora de utilizar Internet lo realizan varias veces al día para sus diferentes actividades sin discriminar el aparato electrónico o la función que realizan; es por esto, que se debe propender a que los servicios de los diferentes operadores sean disponibles y seguros para la navegación.

Realiza usted más compras en línea que compras en tiendas físicas.

45 respuestas

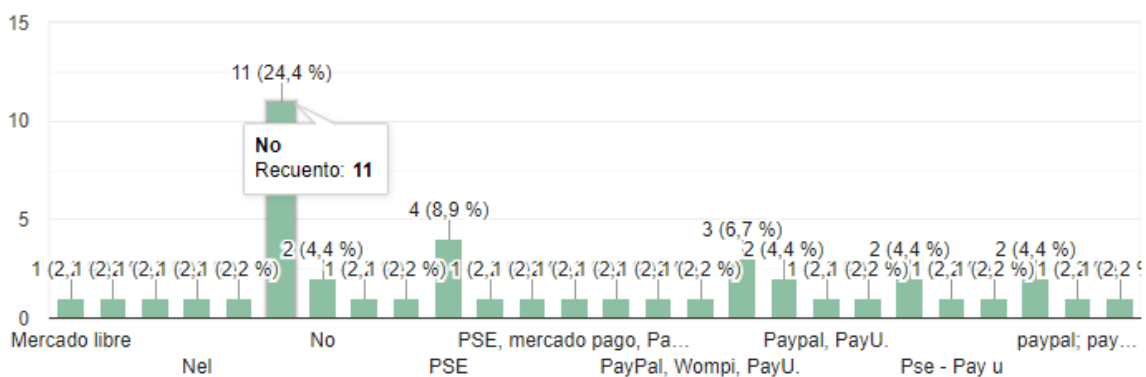


Los participantes, por una leve diferencia, aún continúan realizando compras en establecimientos físicos más que compras en tiendas en línea, para esta decisión pueden influir factores económicos, culturales, tecnológicos entre otros, lo cual puede ser un factor que minimice la expansión de crecimiento de comercio electrónico.

¿Conoce usted alguna pasarela de pago en línea? En caso afirmativo, mencionela.



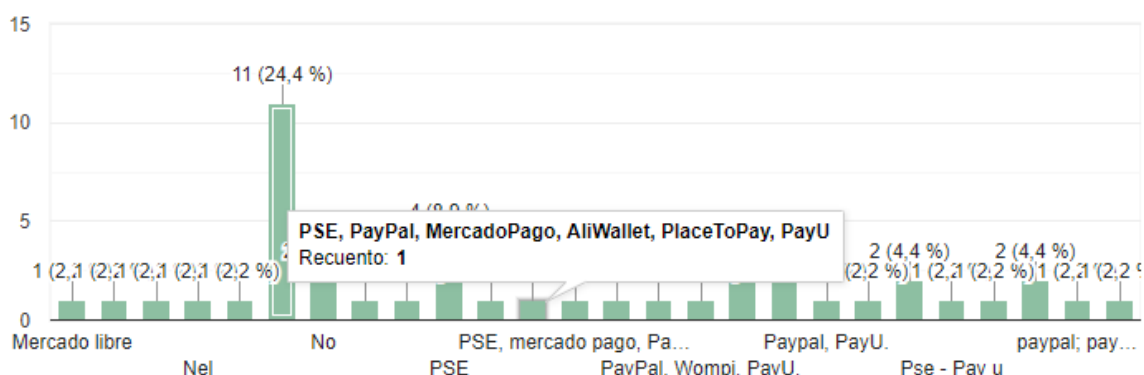
45 respuestas



¿Conoce usted alguna pasarela de pago en línea? En caso afirmativo, mencionela.



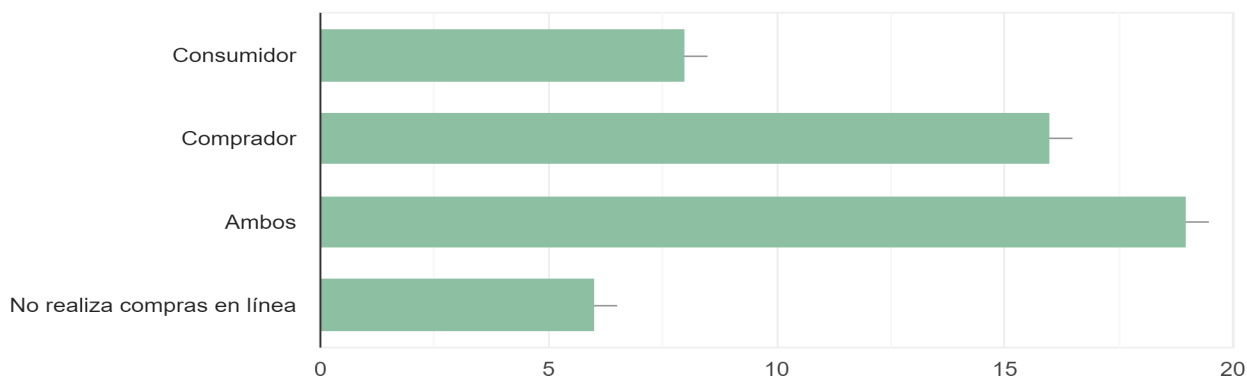
45 respuestas



Se observa que 19 participantes desconocen de pasarelas de pago en línea o no han oído nombrar alguna de ellas, los demás participantes relacionan una o varias de estas que hayan usado o mencionado, entre ellas Nequi, PayU, PSE, PayPal, Wompi, OpenPay entre otras.

¿A la hora de comprar en línea usted qué rol desempeña?

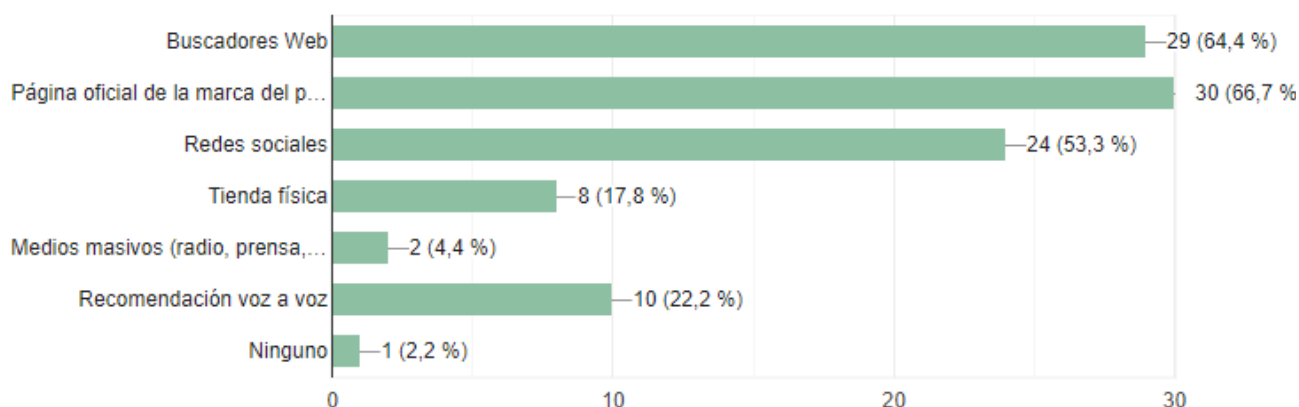
45 respuestas



Se observa que 19 participantes son tanto compradores como consumidores de servicios de comercio electrónico y 6 personas no realizan este tipo de transacciones.

Cuando está interesado en realizar una compra por Internet, ¿Que medio(s) utiliza para indagar sobre el producto que desea adquirir?

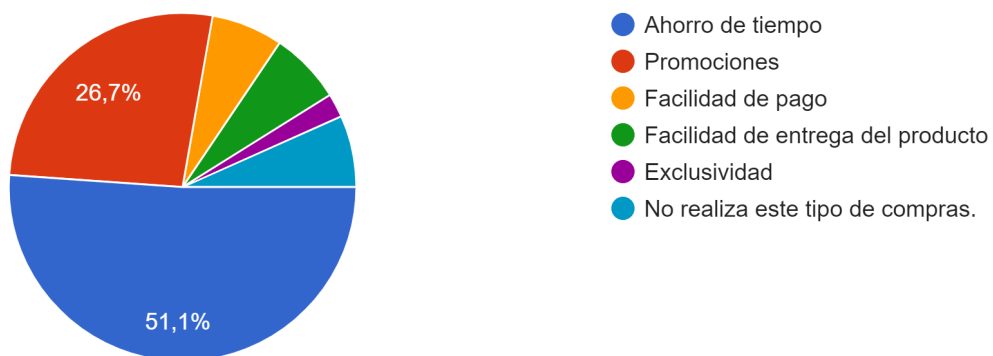
45 respuestas



Los principales medios para indagar sobre un producto que se desea adquirir en línea son los buscadores Web, página oficial de la marca del producto y redes sociales (Facebook, Instagram), sin embargo, se observa que la recomendación voz a voz es una alternativa que aun no pasa de moda y puede ser un medio muy útil a la hora de dar a conocer los beneficios del comercio electrónico y el uso de pasarelas de pago.

¿Qué lo motiva a realizar una compra en línea?

45 respuestas



La principal motivación a la hora de realizar compras en línea son el ahorro de tiempo que esto genera en comparación a las compras en establecimientos físicos, seguido de las promociones que ofrecen los comercios a la hora de usar las pasarelas de pago.

¿Cuál es su principal restricción a la hora de realizar compras en línea?

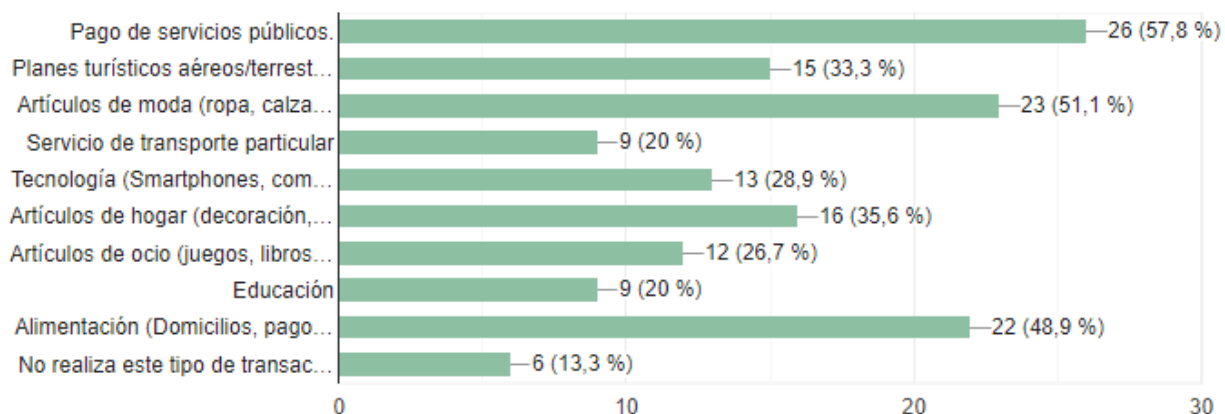
44 respuestas



Como principal restricción a la hora de realizar compras en línea está la incerteza del producto adquirido, seguido de la desconfianza en las pasarelas de pago y proceso de pagos en línea, estas restricciones pueden generar un retroceso en la expansión del comercio electrónico si no se brinda las opciones de seguridad adecuadas.

Si usted es usuario de E-Commerce, habitualmente qué tipo de productos y/o servicios adquiere por Internet

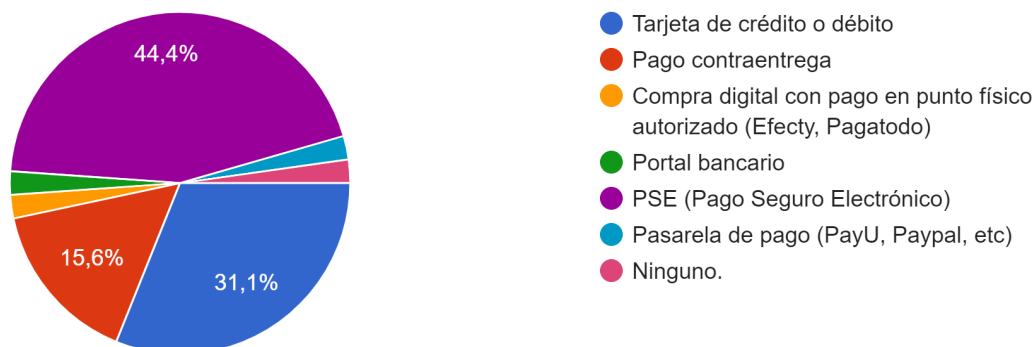
45 respuestas



Entre los principales servicios adquiridos a través del comercio en línea o en el que se requiera utilizar las pasarelas de pago están el pago de servicios públicos, compra de artículos de moda y alimentación, estos servicios son los que cuentan con mayor flexibilidad a la hora de realizar pagos, sea en efectivo o en línea.

Al momento de realizar sus compras en línea, ¿Qué forma de pago utiliza?

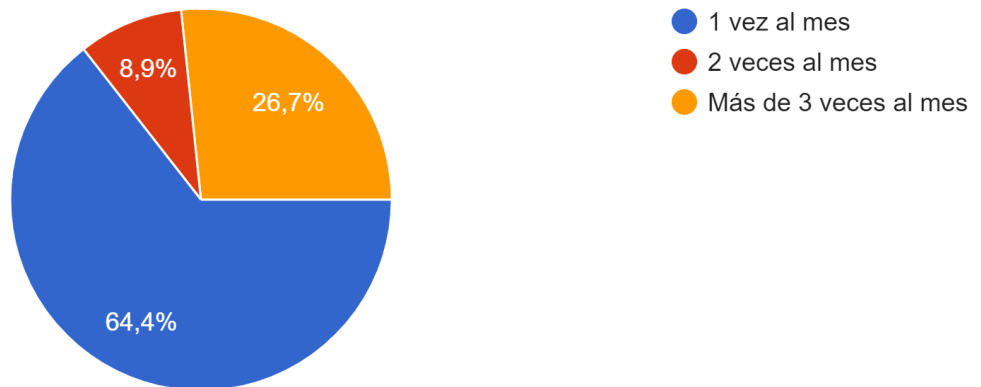
45 respuestas



El uso de PSE es la forma de pago mayormente utilizada cuando se realizan compras en línea, seguido del pago con tarjeta y pago contraentrega.

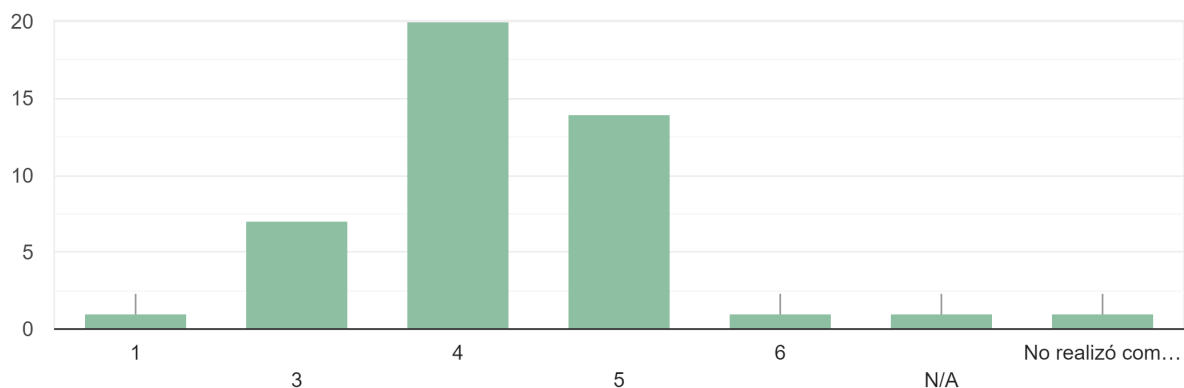
¿Con qué frecuencia realiza sus compras en línea?

45 respuestas



Al momento de realizar compras en línea, se observa un mayor número de compras mensuales en comparación a otros periodos de tiempo, esto cambiando de forma positiva la frecuencia de uso de canales electrónicos.

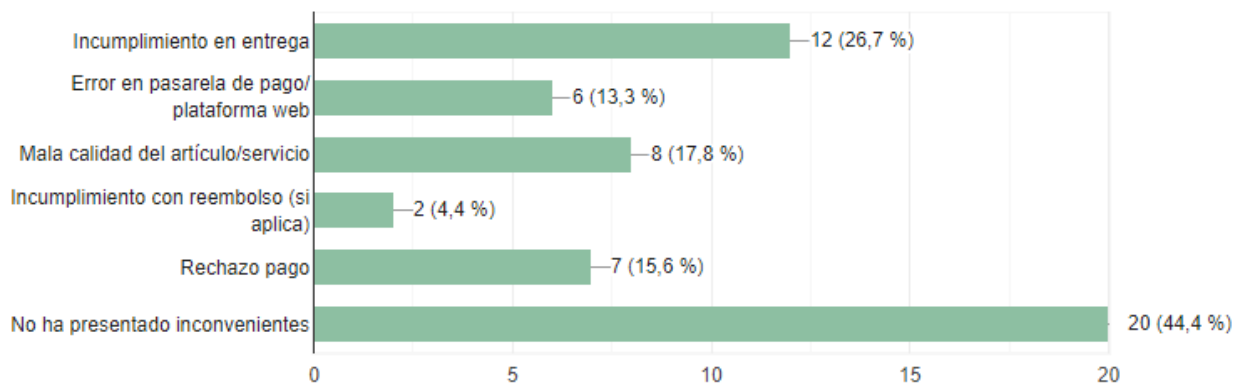
De 1 a 5 donde 1 es muy complicado, 2 complicado, 3 indiferente, 4 sencillo y 5 muy sencillo ¿Qué tan fácil le resulta realizar el proceso de compra ...En caso de que no realice estas compras, indíquelo.
45 respuestas



En este caso, se observa que los participantes que hacen uso de las pasarelas de pago y del comercio electrónico a la hora de realizar el proceso de compra se les facilita estos procesos.

Si ya ha realizado alguna compra en línea, indique qué tipo de inconvenientes presentó con su producto/servicio.

45 respuestas

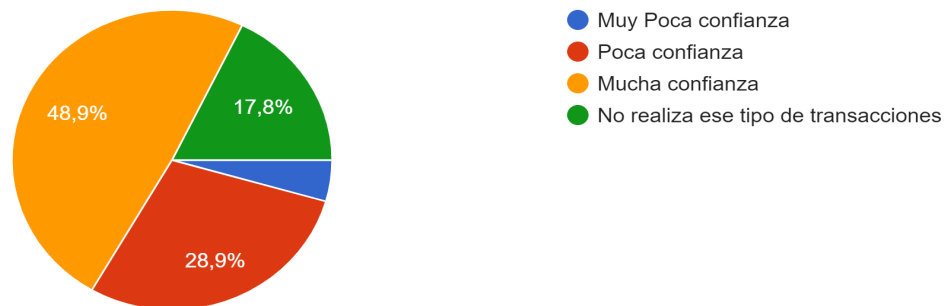


En este caso, se observa que la mayoría de los participantes que hacen uso de las pasarelas de pago y del comercio electrónico no han presentado inconvenientes, pero a quienes sí han

presentado, el mayor inconvenientes es el incumplimiento en entrega, lo cual puede generar una mala experiencia al usuario y desconfianza hacia el establecimiento comercial.

Si usted es usuario de E-Commerce y basado en su experiencia indique el nivel de confianza que le genera realizar transacciones en línea comerciales.

45 respuestas



Si usted es usuario de E-Commerce y basado en su experiencia indique su intención de volver a usar las pasarelas de pago y plataformas en línea para ejecutar transacciones.

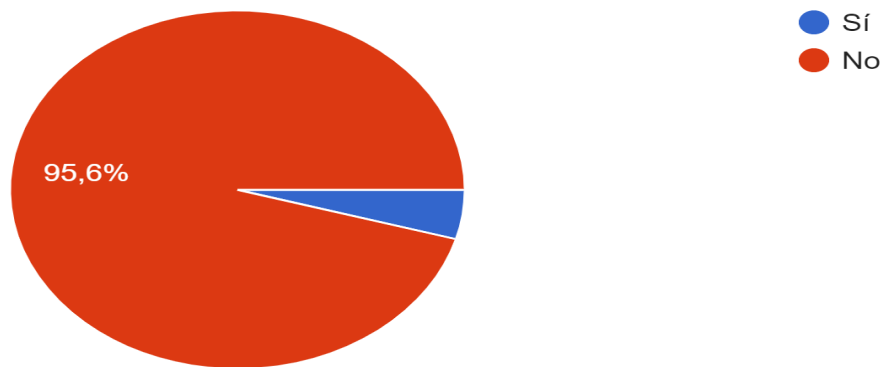
45 respuestas



En este caso, se observa que la mayoría de los participantes que hacen uso de las pasarelas de pago y del comercio electrónico sienten mucha confianza en estas herramientas y otro número significativo tiene poca confianza, por lo cual es objetivo principal buscar que la confianza digital y mecanismos de comercio sean óptimos a la hora de realizar compras en línea.

¿Ha sido víctima de algún delito informático al comprar en línea?

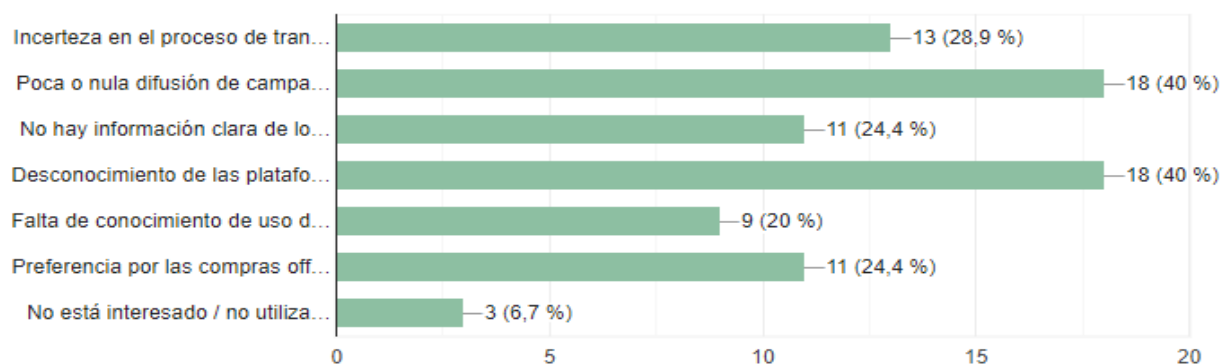
45 respuestas



En este caso, se observa contundentemente que la mayoría de los participantes no han sido víctimas de ciberdelitos, lo cual puede ser un indicador de seguridad de parte de los establecimientos o de los mismos usuarios o que por el contrario no se identifica que delitos o vulnerabilidades se pueden presentar a la hora de realizar pagos en línea.

Indique las razones por las que considera no se ha implementado o se desconoce el uso de pasarelas de pago y plataformas de comercio en línea.

45 respuestas

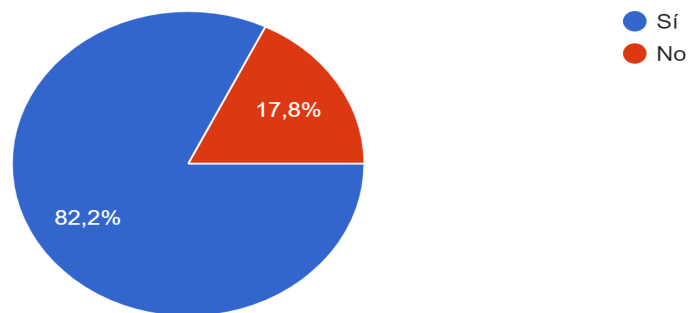


Las principales razones por las cuales se desconoce del uso de las pasarelas de pago y plataformas de comercio en línea obedecen a la poca o nula difusión de campañas antifraude, se

observa que las campañas antifraude están orientadas al sector bancario principalmente. y al desconocimiento de las plataformas por parte de los consumidores y el público en general, esto representa una desventaja significativa al momento de implementar de forma concisa el uso de pasarelas de pago.

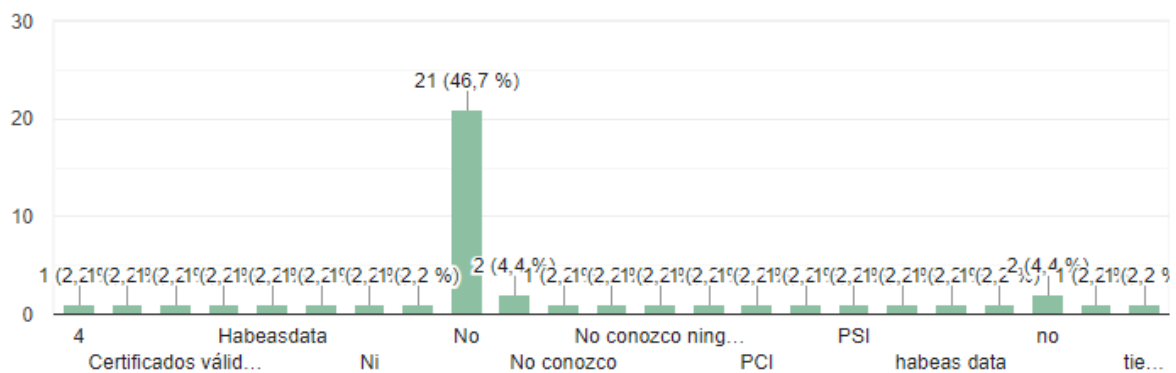
¿Conoce los riesgos cibernéticos a los que se puede exponer al momento de realizar transacciones en pasarelas de pago?

45 respuestas



¿Conoce algún estándar o política de protección de datos y/o ciberseguridad aplicable al uso de pasarelas de pago y comercio en línea? En caso afirmativo, mencionelo.

45 respuestas

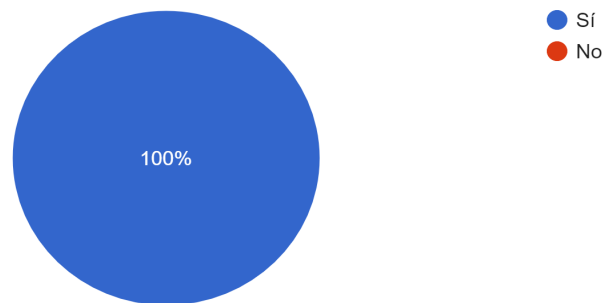


La mayoría de participantes, si bien conocen de los riesgos asociados al uso de servicios de comercio electrónico, desconoce políticas de protección de datos y ciberseguridad, por el

contrario quienes indicaron que conocen alguna de ellas mencionan, los certificados válidos SSL, Habeas Data y el estándar PCI DSS.

¿Le gustaría que los comercios que implementan sistemas de pasarelas de pago y comercio en línea brinden a los usuarios recomendaciones en ...guridad de la información y campañas antifraude?

45 respuestas



Los comercios y pasarelas de pago no cuentan con campañas de concientización fuertes o son nulas de entrada debido a que para los comercios su principal función es vender productos o servicios por lo que no está dentro de su core de negocio transar haciendo que estos temas de programas de aprendizaje en mejores prácticas de seguridad hacia el usuario final con el fin de disminuir el riesgo viene desde el ámbito bancario y se encuentra dirigido en su gran mayoría a sus propios productos (Seguridad en retiros, en compras con tarjeta presente, portal transaccional y banco digital).

Capítulo VI

Conclusiones y Recomendaciones generales para evitar la explotación de las vulnerabilidades y disminuir el riesgo de incurrir en fraude.

La incorporación de canales digitales ha facilitado que el sector bancario y pasarelas de pago estén presentes en los nuevos hábitos de comportamiento de la población a raíz de las medidas de confinamiento y restricciones derivados de la pandemia COVID-19 facilitando las transacciones comerciales y logrando disminuir el riesgo de contagio, dejando en un segundo plano las actividades de índole presencial, entre ellas las relacionadas con compra y venta de productos y servicios.

Teniendo en cuenta que la desconfianza en el uso de las pasarelas de pago es una de las principales restricciones a la hora de implementar un sistema fuerte en comercio electrónico, otro factor a tener en cuenta es la ausencia de mecanismos eficientes y regulación vigente que permitan acceder a los consumidores a herramientas de reclamación para ejercer sus derechos, a pesar que Colombia cuenta con una sólida estructura regulatoria en comparación a otros países, su difusión y conocimiento por parte de la población es baja.

Conociendo las vulnerabilidades y el funcionamiento de las pasarelas de pago además de como es el proceso de ejecución de la transacción el cliente de los e-commerce se siente más confiado a la hora de hacer una compra por internet, por lo tanto se hace necesario generar una campaña de

concientización este el punto de partida para que los clientes sepan como comprobar y diferenciar las estafas, los fraudes y los posibles robos de identidad mediante comprobaciones muy básicas dado que un gran porcentaje de los clientes no tiene claro muchos conceptos tecnológicos o no les interesa conocerlos sino simplemente realizar una compra entonces esta campaña dirigida desde los comercios es esencial en aras de generar confianza que a la final es el pilar número uno cuando una persona va a adquirir algún producto en algún comercio dentro de esta campaña se deben incluir temas como:

- Comprobar de manera de sencilla si esta se trata de una página real o fraudulenta, esto con el fin de disminuir en un porcentaje bastante importante el riesgo dado que muchos de estos se basan en la confianza de las personas cuando acceden en los primeros enlaces o resultados cuando realizan una búsqueda en el navegador, para esto es necesario verificar que la página web tenga incorporado el protocolo https y los certificados digitales válidos y emitidos por fuentes de confianza.
- Fomentar el uso de software antivirus o similares, con el fin de que en los computadores de los usuarios o dispositivos electrónicos existan programas maliciosos que puedan hacerse con los datos que se ven involucrados en la transacción.
- Centralización de canales de comunicación con el único propósito de hacer promoción y difusión al mismo, logrando una clara identificación por parte del consumidor; para evitar y sospechar de todas las comunicaciones que se transmitan por ese único canal de comunicaciones, así mismo enviar capsulas, imágenes o material gráfico donde se exponga de manera clara y sencilla mejores prácticas en seguridad.

- Mejorar el flujo de compra, optimizando los procesos de interacción entre consumidor y comercio, detallando al consumidor sobre lo que está sucediendo al adquirir algún producto o servicio.
- Explicar que en los procesos de compra muchas veces se ven involucradas varias páginas o plataformas haciendo que el cliente desconfíe cuando se realicen redirecciones a sitios que el comercio tiene claro que son necesarios para completar la compra.
- Siempre exponer las certificaciones en los sitios web, en caso de obtener certificaciones como por ejemplo PCI-DSS exponerla en el sitio web donde el usuario pueda ver el logo y además de eso validar el cumplimiento correcto con la norma, sea esta o cualquiera que aplique para esta industria, con el fin de tener un reconocimiento por parte de los usuarios.
- Realizar la omnicanalidad dentro de los procesos de pago, debido a que muchos comercios dependiendo el medio de pago realizan diferentes procesos con diferentes pasarelas de pago, lo ideal es mantener un solo proceso independientemente el medio de pago seleccionado por el usuario, ya que puede generar desconfianza.

Una vez se ejecute correctamente la campaña anteriormente descrita, se verá un aumento considerable en el uso de los canales de internet de los diferentes comercios y de manera inversamente proporcional la disminución de los riesgos y la explotación de estas vulnerabilidades presentadas; por ende la confianza aumenta y los clientes se sentirán más cómodos a la hora de hacer compras, ya que si se añade seguridad a la agilidad y comodidad del comercio electrónico se vuelve una receta prácticamente infalible para hacer de éste un canal aún más fuerte de ventas, para finalizar lo ideal es tomar este presente documento como insumo para cumplir con el objetivo de los comercios y maximizar el uso del e-commerce y que sirva como

pauta para trabajos futuros en los cuales se pueda explorar y ahondar más en los temas descritos y que sean vigentes y aplicables al territorio nacional.

Referencias.

Asobancaria. (2020). *Estado de la ciberseguridad en el sistema financiero colombiano*. OEA.

https://www.asobancaria.com/wp-content/uploads/2020/10/20201014-ASOBANCARIA-2020_compressed.pdf

Barrera Barrera, R., Bravo García, S., & Navarro García, A. (2014). Evaluación de la actitud hacia las compras online: Un estudio realizado en Colombia.

<https://www.researchgate.net/publication/301341692>

Bohórquez Guevara, K. (2019, 22 julio). Conozca cómo operan las distintas alternativas de pasarelas de pago. Diario La República.

<https://www.larepublica.co/finanzas-personales/conozca-como-operan-las-distintas-alternativas-de-pasarelas-de-pago-2887641>

Calvo, J. F. P. (2021). *Principios de seguridad en el comercio electrónico*. RA-MA S.A. Editorial y Publicaciones.

Ceballos Lopez, A., Bautista Garcia, F., Mesa Guzman, L., & Arguez Quintero, C. (2019, octubre). Informe de las tendencias del cibercrimen en Colombia (2019–2020) (N.o 1).

https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf

Comisión de Regulación de Comunicaciones. (2017). El Comercio electrónico en Colombia.

Congreso de Colombia [Ley 527 de 1999]. Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.

Congreso de Colombia [Ley 1266 de 2008]. Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.

Congreso de Colombia [Ley 1480 de 2011]. Por medio de la cual se expide el estatuto del consumidor y se dictan otras disposiciones.

Congreso de Colombia [Ley 1581 de 2012]. Por la cual se dictan disposiciones generales para la protección de datos personales.

Cortés Cortés, M. E., Iglesias León, M., U.A., Universidad Autónoma del Carmen (Campeche). (2004). Generalidades sobre metodología de la investigación (1.a ed.). Universidad Autónoma del Carmen.

http://www.unacar.mx/contenido/gaceta/ediciones/metodologia_investigacion.pdf

Departamento Nacional de Planeación, Ministerio de Comercio, I. y T., Ministerio de Tecnologías de la Información y las Comunicaciones. (2020). *Documento CONPES 4012 - Política Nacional de Comercio Electrónico*.

<https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/4012.pdf>

Medina, R. K. (2021, 28 abril). El crecimiento del e-commerce en Colombia (Análisis 2020).

Branch.

<https://branch.com.co/marketing-digital/el-crecimiento-del-e-commerce-en-colombia-analisis-2020/>

Ministerio de Hacienda y Crédito Público [Decreto 1692 de 2020]. Por medio del cual se modifica el Decreto 2555 de 2010 en lo relacionado con los sistemas de pago de bajo valor.

18 de diciembre de 2020.

<https://dapre.presidencia.gov.co/normativa/normativa/DECRETO%201692%20DEL%2018%20DE%20DICIEMBRE%20DE%202020.pdf>

Organización de los Estados Americanos; Ministerio de Tecnologías de la Información y las Comunicaciones; Banco Interamericano de Desarrollo. (2017). Impacto de los incidentes de seguridad digital en Colombia 2017. 27. <http://dx.doi.org/10.18235/0000843>

Organización de los Estados Americanos & Asobancaria. (2019, octubre). Desafíos del riesgo cibernético en el sector financiero para Colombia y América Latina.

<https://www.oas.org/es/sms/cicte/docs/Desafios-del-riesgo-cibernetico-en-el-sector-financiero-para-Colombia-y-America-Latina.pdf>

Organización de los Estados Americanos & Asobancaria. (2020). Estado de la ciberseguridad en el Sistema Financiero Colombiano. 85–86.

https://www.asobancaria.com/wp-content/uploads/2020/10/20201014-ASOBANCARIA-2020_compressed.pdf

Portafolio.co. (2021a, junio 14). Así puede seleccionar una pasarela de pago confiable para su negocio.

<https://www.portafolio.co/negocios/empresas/asi-puede-seleccionar-una-pasarela-de-pago-confiable-para-su-negocio-552951>

Smith, G. E. (2003). *Control and security of E-Commerce*. Wiley.

Venegas Loaiza, A. (2019, 15 febrero). El número de pasarelas de pago en línea en Colombia ha crecido 53,9%. Diario La República.

<https://www.larepublica.co/internet-economy/el-numero-de-pasarelas-de-pago-en-linea-en-colombia-ha-crecido-539-2828821>

Villalba, D. (2021, 26 enero). Conoce los tipos de E-commerce. Pragma.

<https://www.pragma.com.co/blog/conoce-los-tipos-de-ecommerce>