UNIVERSIDAD & SOCIEDAD

Fecha de presentación: diciembre, 2024
Fecha de aceptación: febrero, 2025
Fecha de publicación: marzo, 2025

# CIBERSEGURIDAD

## Y PROTECCIÓN DE DATOS EN E-COMMERCE

## CYBERSECURITY AND DATA PROTECTION IN E-COMMERCE

Johny Teodoro Coellar Solano[1*]
E-mail: johny.coellar.08@est.ucacue.edu.ec
ORCID: https://orcid.org/0009-0005-9525-2036
Diego Marcelo Cordero Guzmán[1]
E-mail: dcordero@ucacue.edu.ec
ORCID: https://orcid.org/0000-0003-2138-2522
Juan Carlos Erazo Álvarez[1]
E-mail: jcerazo@ucacue.edu.ec
ORCID: https://orcid.org/0000-0001-6480-2270
José Alberto Rivera Costales[1]
E-mail: jriverac@ucacue.edu.ec
ORCID: https://orcid.org/0000-0001-9965-081X
[1]Universidad Católica de Cuenca. Ecuador.
*Autor de correspondencia

Cita sugerida (APA, séptima edición):

Coellar Solano, J. T., Cordero Guzmán, D. M., Erazo Álvarez, J. C. & Rivera Costales, J. A. (2025 Ciberseguridad y protección de datos en e-commerce. ***Universidad y Sociedad, 17***(2), e4988.

### RESUMEN

La ciberseguridad protege la información mediante cifrado, gestión de contraseñas, políticas de acceso y firewalls contra amenazas externas. Su objetivo es valorar el impacto de las estrategias de ciberseguridad y protección de datos en la confianza de los consumidores y su decisión de compra en plataformas de e-commerce en el sector de consumo de helado en la ciudad de Cuenca. Se utilizó una metodología mixta, combinando encuestas cualitativas y cuantitativas para captar la percepción de 91 usuarios. Los resultados muestran que el 57.14% de los encuestados considera efectivas las medidas de protección de datos, mientras que un 82.42% otorga gran importancia a la transparencia en el manejo de su información. La investigación revela una correlación positiva entre la percepción de seguridad en línea y la disposición de compra, resaltando que los consumidores confían más en plataformas con robustas medidas de ciberseguridad. Se debe mejorar las prácticas de seguridad y mantener una comunicación transparente son claves para fomentar la confianza y lealtad de los usuarios en el e-commerce.

Palabras clave: Seguridad de los datos, Informática y desarrollo, Tecnología de la información, Datos estadísticos, Usuario de información.

### ABSTRACT

Cybersecurity protects information through encryption, password management, access policies and firewalls against external threats. Its objective is to assess the impact of cybersecurity and data protection strategies on consumer confidence and purchasing decisions in e-commerce platforms in the ice cream consumption sector in the city of Cuenca. A mixed methodology was used, combining qualitative and quantitative surveys to capture the perception of 91 users. The results show that 57.14% of respondents consider data protection measures to be effective, while 82.42% attach great importance to transparency in the handling of their information. The research reveals a positive correlation between the perception of online security and willingness to purchase, highlighting that consumer trust platforms with robust cybersecurity measures more. Improving security practices and maintaining transparent communication are key to fostering user trust and loyalty in e-commerce.

Keywords: Data security, Computing and development, Information technology, Statistical data, Information user.

## INTRODUCCIÓN

La ciberseguridad y la protección de datos se han convertido en componentes esenciales para garantizar la integridad y confidencialidad de la información en la era digital. Las medidas de ciberseguridad incluyen la implementación de protocolos de cifrado, la gestión adecuada de contraseñas y la adopción de políticas de acceso restringido, además del uso de firewalls y sistemas de detección de intrusiones para proteger redes y sistemas contra amenazas externas. A su vez, la protección de datos busca salvaguardar la información personal y sensible mediante el cumplimiento de normativas, que exige el consentimiento explícito de los usuarios para el tratamiento de sus datos y el derecho de estos a acceder, rectificar y eliminar su información. El enfoque efectivo de ciberseguridad combina tanto la prevención como la detección de amenazas, y la formación continua de los usuarios es clave para reducir riesgos humanos.

Ecuador registra más de 12 millones de ciberataques durante el 2023, según un informe del Ministerio de Telecomunicaciones. Este aumento en las amenazas ha impulsado la inversión en seguridad digital en diversos sectores, incluidos alimentos y retail. El sector de consumo de helados en Ecuador, como otros sectores alimentarios, enfrenta crecientes desafíos en ciberseguridad debido a la digitalización de las operaciones y la adopción del comercio electrónico. Las empresas de helados que manejan plataformas de ventas en línea y servicios de entrega a domicilio están expuestas a riesgos relacionados con el robo de datos de clientes, fraudes en pagos y ataques a sus sistemas de información. En este contexto, la protección de datos financieros y personales de los consumidores de helados es crucial para mantener la confianza del cliente y cumplir con las normativas locales, como la Ley de Protección de Datos Personales de Ecuador (Merchán, 2024).

Cabe considerar que, en la provincia del Azuay, el sector de consumo de helados ha experimentado un crecimiento en el uso de plataformas digitales, especialmente en servicios de entrega a domicilio y ventas online. Este incremento en la digitalización ha planteado desafíos en ciberseguridad, ya que muchas de las pequeñas y medianas empresas (PYMEs) de helados no cuentan con sistemas robustos de protección de datos. La implementación de medidas de ciberseguridad, como el cifrado de datos y la autenticación de dos factores, es limitada, lo que las hace vulnerables a ataques cibernéticos, especialmente en la gestión de pagos electrónicos y la protección de la información de los clientes. En esta perspectiva, reportes locales señalan que un buen porcentaje de las empresas en la región no han implementado políticas formales de protección de datos, porque no consideran que los riesgos cibernéticos sea algo prioritario, lo que resalta la necesidad de fortalecer las medidas de seguridad digital en este sector (Ecuador. Ministerio de Telecomunicaciones, 2022).

En la ciudad de Cuenca, el sector de consumo de helados, compuesto mayormente por pequeñas empresas, ha incrementado el uso de redes sociales y plataformas de comercio electrónico para impulsar las ventas, lo que ha expuesto a estos negocios a riesgos de ciberseguridad. La mayoría de estas empresas carecen de infraestructura tecnológica adecuada para proteger la información sensible de sus clientes, como datos personales y financieros. Un estudio reciente de la Universidad de Cuenca reveló que un 60% de los pequeños negocios en la ciudad, incluyendo heladerías, no cuentan con sistemas de seguridad avanzados, como cifrado de datos o firewalls, lo que los deja vulnerables ante ataques como el phishing y fraudes electrónicos. En ese mismo contexto, señala que Cuenca ha sido una de las ciudades con más incidentes de seguridad digital en el último año, afectando principalmente a pequeñas empresas (Peralta & Aguilar, 2021).

La confianza de los consumidores es un factor clave en la decisión de compra, especialmente en entornos digitales. Cuando los clientes sienten que sus datos están protegidos y que las empresas son transparentes en sus prácticas, es más probable que realicen compras repetidas. La confianza se construye a través de la reputación de la marca, la calidad del producto, las reseñas y la experiencia del cliente en plataformas digitales seguras (Kumar, 2024).

El comportamiento del consumidor está influenciado por la percepción de riesgo y seguridad. Los consumidores tienden a evitar transacciones con empresas que parecen vulnerables a fraudes o que no protegen adecuadamente su información. En lo esencial, factores emocionales como la familiaridad con la marca y la facilidad de uso de las plataformas influyen en la decisión de compra. En mercados de consumo como el de helados, construir la confianza del cliente es clave para el éxito, se debe mantener una comunicación clara y honesta, ofreciendo información precisa sobre productos y servicios. Es cierto, la resolución rápida de problemas es esencial para satisfacer a los consumidores, mostrando un compromiso proactivo en caso de inconvenientes. La atención personalizada es otro factor crucial, al adaptar productos y servicios a las necesidades individuales, las marcas pueden generar mayor lealtad en el competitivo mercado del helado (Docusign Inc, 2023).

La confianza es esencial para las relaciones comerciales, especialmente en la era digital, donde los consumidores no tienen contacto físico con los productos antes de

comprarlos. En este contexto, la confianza depende de la transparencia, el cumplimiento de promesas y la capacidad de generar seguridad en las transacciones. La confianza influye en el comportamiento del consumidor al aumentar la predisposición a la compra recurrente y la recomendación. También actúa como un diferenciador clave en un entorno competitivo, contribuyendo a la retención de clientes y a la reducción del abandono en procesos de compra online (Vela et al., 2023).

De igual manera, la confianza digital reduce la incertidumbre en las transacciones online y fomenta relaciones a largo plazo. Evidentemente, influye en el comportamiento del consumidor, alentando la participación en programas de fidelización y compartiendo experiencias positivas en redes sociales. Facilita la toma de decisiones al reducir el esfuerzo cognitivo necesario para evaluar opciones de compra. A través de una experiencia confiable y transparente, las empresas no solo aseguran ventas, sino también la lealtad del consumidor en un entorno digital altamente competitivo (Narciso, 2024).

Cabe considerar que, la confianza se clasifica en tres tipos: confianza cognitiva, basada en la capacidad percibida de la empresa para cumplir sus promesas; confianza afectiva, relacionada con las emociones positivas que genera la marca; y confianza normativa o conductual, vinculada a la percepción de que la empresa opera de manera ética y responsable. En un contexto digital, donde los consumidores valoran la ética y la transparencia, las empresas que demuestran responsabilidad en su operación tienen más probabilidades de generar una confianza duradera.

En cuanto a su construcción, la confianza se desarrolla en cada interacción con el cliente. Desde el primer contacto, la consistencia y transparencia son claves para generar una relación de confianza. La personalización de la experiencia también contribuye a este proceso, ya que los clientes valoran que la empresa entienda sus necesidades y les ofrezca soluciones adaptadas. Una experiencia fluida, coherente y personalizada en todos los canales de venta ayuda a reforzar la confianza y establecer una relación sólida con el cliente.

Habida cuenta, los desafíos de construir confianza en la era digital incluyen la sobrecarga de información, el aumento de los ciberataques y las expectativas cada vez más altas de los consumidores. Para mantener la confianza, las empresas deben proteger los datos de sus usuarios y adaptarse rápidamente a las necesidades cambiantes del mercado. La transparencia y la capacidad de respuesta ante crisis también son esenciales para preservar la confianza y evitar que los consumidores cambien a la competencia.

La ciberseguridad es un enfoque integral que busca proteger de manera completa los datos, sistemas, redes y usuarios frente a las crecientes amenazas en el entorno digital. En un mundo donde la información es uno de los activos más valiosos y vulnerables, esta estrategia busca abarcar todos los frentes de seguridad, desde la protección de dispositivos individuales hasta la seguridad en la nube y los sistemas empresariales. Este concepto implica la implementación de diversas tecnologías, políticas y prácticas que protejan los datos desde todos los ángulos posibles, asegurando la continuidad y estabilidad de las operaciones tanto personales como empresariales.

Este enfoque completo de ciberseguridad es fundamental para evitar ataques cibernéticos, violaciones de datos y otros tipos de incidentes que pueden comprometer la confidencialidad, integridad y disponibilidad de la información. El objetivo principal de la ciberseguridad es crear un ecosistema seguro que permita el funcionamiento fluido de los procesos digitales, garantizando que tanto los usuarios como las organizaciones puedan operar en el entorno digital con el menor riesgo posible. Esto es especialmente importante en la actualidad, donde el uso de la tecnología está cada vez más extendido y las amenazas son más sofisticadas y constantes (Calle et al., 2024).

La ciberseguridad se puede clasificar en diferentes áreas que cubren varios niveles de protección. Una de las áreas más importantes es la seguridad de la información, que asegura que los datos sean gestionados y almacenados de manera segura, garantizando que solo las personas autorizadas puedan acceder a ellos. La seguridad de redes es otra parte esencial, encargada de proteger la infraestructura de red, como routers y servidores, evitando que los hackers puedan penetrar en los sistemas empresariales. También es crucial la seguridad en la nube, que protege los datos almacenados en servidores externos, y la seguridad de dispositivos móviles, que se enfoca en la protección de smartphones y tablets, cada vez más utilizados para manejar información sensible (Kashyap & Chaudhary, 2023).

La aplicación de un enfoque de ciberseguridad implica una serie de estrategias y tecnologías que abarcan varios niveles de protección. En el ámbito empresarial, se suelen implementar medidas como firewalls, antivirus avanzados, sistemas de detección de intrusos (IDS) y cifrado de datos. Estas herramientas son esenciales para asegurar que la información esté protegida tanto en reposo como en tránsito. Es por eso que, en muchas organizaciones se utilizan políticas de seguridad rigurosas que incluyen la gestión de parches y actualizaciones, asegurando que todos los sistemas estén protegidos contra vulnerabilidades conocidas.

El entrenamiento y la concienciación del personal también son componentes clave de la ciberseguridad, dado que el error humano es uno de los mayores riesgos en la seguridad informática, las organizaciones deben capacitar a sus empleados para reconocer amenazas como el

phishing, que sigue siendo una de las principales causas de violaciones de datos. Por esto, las auditorías de seguridad y las evaluaciones de vulnerabilidades ayudan a las organizaciones a identificar puntos débiles en sus sistemas, permitiendo aplicar mejoras antes de que los atacantes puedan aprovecharlas. Todo esto permite blindar los datos en un entorno digital donde los riesgos son constantes y evolucionan rápidamente.

No solo las grandes empresas pueden beneficiarse de un enfoque de ciberseguridad; los consumidores y pequeñas empresas también pueden implementar medidas que protejan sus datos. En el ámbito personal, una buena estrategia de seguridad puede comenzar por el uso de contraseñas fuertes y únicas, la activación de la autenticación de múltiples factores en todas las cuentas importantes y el uso de soluciones de seguridad como antivirus y firewalls. Por esto, es esencial realizar copias de seguridad periódicas de los datos, ya sea en la nube o en dispositivos físicos, para evitar la pérdida de información ante un ataque o fallo de hardware. Para las pequeñas y medianas empresas (PYMES), que muchas veces no cuentan con grandes equipos de seguridad informática, es crucial implementar medidas básicas pero efectivas. Estas pueden incluir la segmentación de redes para evitar que una brecha en un área afecte a toda la organización, con estas acciones, se puede reducir el riesgo de ser víctimas de ciberataques y asegurar la protección de sus datos y los de sus clientes (S2 Grupo, 2024).

A pesar de las numerosas ventajas del enfoque de ciberseguridad, su implementación no está exenta de desafíos. Uno de los principales problemas es el costo asociado a las tecnologías avanzadas y al personal especializado necesario para mantener los sistemas seguros. Las pequeñas organizaciones, en particular, pueden encontrar difícil justificar grandes inversiones en ciberseguridad, lo que las hace más vulnerables a los ataques. Por consiguiente, el rápido ritmo de la evolución tecnológica significa que las amenazas también están en constante cambio, lo que obliga a las empresas a estar siempre un paso adelante y actualizar constantemente sus defensas.

Otro desafío importante es la complejidad de la integración de diversas herramientas de seguridad. Muchas veces, las organizaciones cuentan con múltiples soluciones que no están bien coordinadas, lo que puede crear brechas de seguridad. Para superar este problema, es necesario adoptar una estrategia unificada que combine todas las tecnologías y prácticas bajo una única visión de seguridad. A medida que los ciberataques se vuelven más sofisticados, también crece la necesidad de un enfoque integral y coordinado que abarque todos los aspectos de la protección digital (Gracy, 2024).

Por consiguiente, el problema que se genera en el presente artículo es ¿Cómo influyen las medidas de ciberseguridad y protección de datos en la confianza y comportamiento de los consumidores en plataformas de e-commerce? Por lo que, el objetivo que se plantea es de valorar el impacto de las estrategias de ciberseguridad y protección de datos en la confianza de los consumidores y su decisión de compra en plataformas de e-commerce en el sector de consumo de helado en la ciudad de Cuenca.

## MATERIALES Y MÉTODOS

El paradigma de la investigación mixta combina métodos cualitativos y cuantitativos que ayudó a lograr una comprensión más completa de un fenómeno. Este enfoque permitió a los investigadores beneficiarse tanto de la profundidad proporcionada por los datos cualitativos como de la exactitud de los datos cuantitativos, lo que mejoró el análisis y la interpretación de los resultados. Es particularmente útil en estudios que requieren una exploración detallada del fenómeno, mientras se evaluaron de manera profunda también se midieron las variables específicas (Pimienta & De la Orden, 2017).

Es importante señalar que este enfoque facilitó la validación de resultados a través de la triangulación, mejorando la credibilidad. Su flexibilidad permite a los investigadores ajustar los métodos según las necesidades de cada fase del estudio, logrando un diseño más sólido. También brindó amplitud como profundidad en la recolección de datos, siendo útil en áreas complejas. La interpretación se enriqueció al combinar ambos tipos de datos, mejorando la toma de decisiones (Bernal, 2010).

Los métodos de investigación fueron esenciales para obtener resultados precisos, estructurando el conocimiento y comprendiendo fenómenos complejos de manera rigurosa. El método analítico-sintético se basó en descomponer un fenómeno o problema en sus elementos constitutivos para comprender mejor cada una de sus partes, una vez analizadas en detalle, volver a integrarlas para formar una visión global que permitió entender cómo interactúan y contribuyen al fenómeno en su totalidad.

El método inductivo-deductivo, por su parte, combinó dos enfoques complementarios: el inductivo, que parte de observaciones específicas para generalizar y formular teorías o hipótesis a partir de datos empíricos y el deductivo que parte de teorías generales para aplicarlas a situaciones particulares con el fin de probar su validez. El método histórico-lógico se enfocó en analizar fenómenos dentro de su contexto temporal, observando cómo han evolucionado a lo largo del tiempo y relacionándolos con otros eventos o procesos, utilizando tanto el análisis histórico como el razonamiento lógico para identificar dinámicas de cambio.

El método descriptivo tiene como objetivo describir las características de un fenómeno sin manipular variables,

lo que permitió obtener una visión clara y detallada de la situación actual, siendo especialmente útil en estudios exploratorios para identificar patrones y tendencias. Estos métodos fueron fundamentales para la investigación científica y pudieron ser aplicados de manera combinada, dependiendo de los objetivos específicos del estudio y de la naturaleza del fenómeno a investigar.

Las técnicas de investigación fueron herramientas fundamentales que permitieron recopilar datos de manera sistemática, facilitando el análisis. La encuesta fue una técnica para recolectar datos que utilizaron un cuestionario estructurado y permitió obtener información de un gran número de personas, siendo útil principalmente en investigaciones cuantitativas. Su principal ventaja es que estandariza las respuestas, lo que facilita su análisis estadístico y la comparación entre los encuestados. Resulta claro que, puede ser administrada de diversas maneras, como de forma presencial, telefónica o en línea, lo que le otorga un gran alcance. Sin embargo, su principal limitación radica en la profundidad de las respuestas, ya que muchas veces se emplean preguntas cerradas y la calidad de los datos depende de la claridad con la que se formulan las preguntas (Hernández & Mendoza, 2018).

## RESULTADOS Y DISCUSIÓN

Para comprender las expectativas y comportamientos de los consumidores en relación con la ciberseguridad y la protección de datos en plataformas de comercio electrónico, se lleva a cabo una encuesta a 91 usuarios. A través de este análisis, se busca obtener una visión más clara sobre las preocupaciones, expectativas y el nivel de confianza que los usuarios depositan en las prácticas de protección de datos, lo cual es crucial para el fortalecimiento de la seguridad en el entorno digital y el desarrollo de relaciones comerciales basadas en la transparencia.

El presente estudio busca explorar la correlación entre la preocupación de los usuarios por su seguridad, en línea y la importancia que estos otorgan a la ciberseguridad. Los resultados resaltan la importancia de fortalecer la conciencia sobre la ciberseguridad para fomentar comportamientos más cautelosos y seguros en línea. En la tabla 1, se presenta dichos resultados.

Tabla 1: Correlación entre la preocupación de la seguridad de compras en línea y la importancia de la ciberseguridad.

| | **Preocupación seguridad en línea** | | | |
|---|---|---|---|---|
| **Importancia ciberseguridad** | **Muy frecuentemente** | **Frecuentemente** | **Ocasionalmente** | **Total** |
| Muy Importante | 60 | 17 | 6 | 83 |
| Moderadamente Importante | 2 | 0 | 0 | 2 |
| Importante | 1 | 1 | 4 | 6 |
| Total | 63 | 18 | 10 | 91 |

Fuente: elaboración propia.

El análisis de la tabla muestra una clara tendencia de que las personas que consideran la ciberseguridad como muy importante tienden a preocuparse más por la seguridad en línea. Un número considerable de individuos dentro de este grupo reporta estar muy frecuentemente preocupados por su seguridad en línea. En cambio, aquellos que consideran la ciberseguridad como importante o moderadamente importante muestran un menor nivel de preocupación por la seguridad en línea, apareciendo en menor número en las categorías de preocupación frecuente o muy frecuente. Esto sugiere una relación positiva entre la percepción de importancia de la ciberseguridad y el nivel de preocupación por la seguridad en línea, destacando que, a mayor importancia otorgada a la ciberseguridad, mayor es la frecuencia con la que las personas se preocupan por su seguridad en línea.

La tabla anterior describe la correlación entre las variables dependiente e independiente de la investigación (Preocupación seguridad en línea y la importancia de la ciberseguridad). Así mismo, el análisis de las respuestas sobre la percepción de la efectividad de las medidas de protección de datos en sitios de e-commerce revela que la mayor parte de los encuestados tiene una opinión positiva o neutra al respecto. Un 29.67% de los participantes considera que las medidas son algo efectivas, mientras que un 27.47% cree que son muy efectivas, lo que da un total del 57.14% de opiniones favorables. En cambio, un 28.57% mantiene una postura neutral sobre la efectividad, esto indica que, aunque no están completamente convencidos, tampoco perciben fallos importantes. Solo el 13.19% de los encuestados considera que las medidas son poco efectivas, y una mínima parte, el 1.10%, opina que no son efectivas en

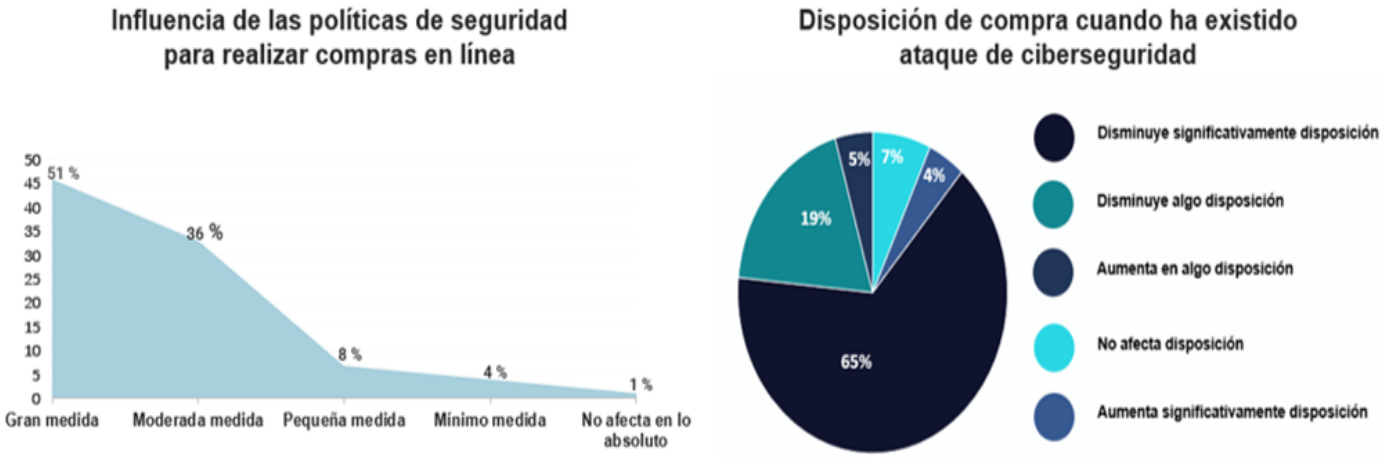
absoluto. No hubo respuestas ausentes, lo que refleja que los 91 encuestados dieron su opinión completa, esto indica que una mayoría significativa confía en la efectividad de las medidas de protección de datos implementadas en las plataformas de e-commerce que utilizan, aunque existe una minoría que aún ve espacio para mejorar.

Por consiguiente, en la figura 1 se analiza la relación entre la percepción de seguridad en el comercio electrónico y la disposición de compra, a mayor percepción de seguridad, mayor es la intención de compra, destacando la influencia de la protección de datos. Incluso en situaciones de seguridad moderada, la disposición a comprar persiste.

La figura 1 describe la correlación entre las variables dependiente e independiente de la investigación (Disposición de compra y seguridad en e-commerce). El análisis de la figura muestra una relación significativa entre la percepción de seguridad en el comercio electrónico y la disposición de compra de los usuarios. La mayoría de los encuestados cuya disposición aumenta notablemente tienen una alta percepción de seguridad en las transacciones en línea.

A medida que disminuye esta percepción, también se reduce la disposición a comprar, aunque no de manera tan marcada como en los casos de mayor seguridad. Existen algunos casos donde la disposición de compra disminuye, pero en general, la percepción de seguridad parece influir positivamente. Incluso en situaciones de seguridad moderada o mínima, sigue existiendo cierta disposición de compra, aunque menos pronunciada. Pocos participantes indican que la seguridad no afecta en absoluto su disposición a comprar, lo que refuerza la idea de que la percepción de seguridad es un factor clave para fomentar la intención de compra en entornos de comercio electrónico.

Fig 1. Dashboard de: Influencia de la seguridad en e-commerce para el comportamiento del consumidor y la disposición de compra.




Fuente: elaboración propia.

En un mundo cada vez más digital, la protección de datos personales se ha convertido en una preocupación fundamental para los usuarios de plataformas de e-commerce. Este análisis explora la relevancia que los consumidores otorgan al buen manejo de su información personal. A continuación, en la tabla 2 se presenta los resultados.

Tabla 2. Importancia de que una plataforma de e-commerce sea transparente en la protección de datos personales.

| Relevancia de la protección de los datos personales | Frecuencia | Porcentaje | Porcentaje Válido | Porcentaje Acumulado |
|---|---|---|---|---|
| Muy relevante | 75 | 82.42 | 82.42 | 82.42 |
| Algo relevante | 10 | 10.98 | 10.98 | 93.41 |
| Poco relevante | 1 | 1.10 | 1.10 | 94.51 |
| Neutro | 5 | 5.50 | 5.50 | 100.00 |
| Ausente | 0 | 0.00 | | |
| Total | 91 | 100.00 | | |

Fuente: elaboración propia.

La tabla describe que tan relevante es para los consumidores, que una plataforma tenga transparencia en el manejo y protección de datos personales. El análisis de los resultados sobre la relevancia de la transparencia en el manejo y protección de datos por parte de las plataformas de e-commerce muestra que la mayoría de los encuestados considera que este factor es muy relevante, lo que subraya la alta preocupación de los usuarios por la seguridad y la gestión de su información personal. Un grupo adicional lo encuentra algo relevante, lo que eleva considerablemente el número de respuestas positivas.

Solo un pequeño porcentaje de los participantes observa este tema como poco relevante, mientras que otro grupo se mantiene neutral al respecto. No hubo respuestas ausentes, lo que indica un interés generalizado en la pregunta. La mayoría de los encuestados otorgan importancia a la transparencia en la protección de sus datos personales, lo que evidencia una expectativa clara hacia las plataformas de e-commerce de ser transparentes y responsables en su gestión de la información.

Diversos estudios coinciden en que una mayor conciencia sobre los riesgos en línea lleva a una mayor preocupación y a la adopción de medidas preventivas por parte de los usuarios.

Medina et al. (2024), también resaltan la importancia de identificar vulnerabilidades en los entornos digitales. En el contexto del comercio electrónico, los usuarios manifiestan inquietudes sobre la protección de datos, lo que refleja una preocupación generalizada por las vulnerabilidades de las plataformas. Tanto en México como en otros estudios, se destaca que la seguridad de la información es un factor clave para generar confianza en las transacciones en línea.

Por otro lado, Gordillo (2024), observa que, aunque las MiPymes del sector terciario en Fusagasugá (Colombia) muestran interés por la ciberseguridad, carecen de un enfoque claro en la protección de datos. En sectores como los gastrobares, se evidencian importantes brechas en la implementación de políticas de seguridad, mientras que solo una minoría de las empresas de comida rápida adopta estrategias adecuadas para mitigar los riesgos cibernéticos. A pesar de que estos sectores reconocen la importancia de la ciberseguridad, la falta de protocolos sólidos subraya la necesidad de una mayor concienciación y adopción de medidas preventivas.

Rueda (2020), señala que la ciberseguridad es un tema central en la confianza del consumidor, ya que los usuarios expresan una fuerte preocupación por la protección de sus datos personales. En Ecuador, tanto a nivel institucional como gubernamental, existe una creciente preocupación por las amenazas a la ciberseguridad, lo que refleja la necesidad de proteger el entorno digital para evitar daños tanto a individuos como a organizaciones.

En cuanto al comercio electrónico, los consumidores valoran especialmente la transparencia en la protección de datos, lo que influye directamente en su comportamiento de compra. Meléndez & Abrego (2021), concluyen que la confianza en las medidas de protección de datos es un factor determinante en la decisión de compra en línea. De igual manera, se resalta que una percepción positiva de la seguridad en un sitio web está directamente relacionada con una mayor disposición a realizar compras. Incluso cuando la percepción de seguridad es moderada, los consumidores mantienen su intención de compra, lo que subraya la relevancia del factor de seguridad.

Los estudios coinciden en que la transparencia y la protección adecuada de los datos personales no solo fortalecen la confianza de los usuarios, sino que también son un diferenciador importante al momento de elegir entre diferentes plataformas de comercio electrónico.

## CONCLUSIONES

Existe una correlación positiva entre la importancia que los usuarios otorgan a la ciberseguridad y su preocupación por la seguridad en línea. A medida que los usuarios valoran más la ciberseguridad, su nivel de preocupación por las vulnerabilidades y amenazas en el entorno digital aumenta, lo cual refuerza la necesidad de una mayor concienciación sobre estos riesgos.

Un porcentaje significativo de los encuestados, el 57.14%, percibe que las medidas de protección de datos en las plataformas de comercio electrónico son efectivas o muy efectivas, lo que sugiere que existe una confianza considerable en las prácticas actuales. Sin embargo, el 13.19% de los usuarios aún percibe que estas medidas son poco o nada efectivas, lo que destaca la necesidad de mejorar continuamente las estrategias de protección.

La percepción de seguridad en una plataforma de comercio electrónico influye directamente en la disposición de los usuarios a realizar compras. Aquellos que perciben un entorno de seguridad robusto muestran una mayor disposición a comprar, mientras que, en situaciones de seguridad moderada, aunque la intención de compra disminuye, sigue existiendo.

La mayoría de los encuestados (82.42%) considera que la transparencia en la protección de datos personales es un factor muy relevante al utilizar plataformas de e-commerce. Esto refleja una expectativa clara de que las plataformas deben ser responsables y transparentes en el manejo de la información, lo que a su vez puede aumentar la confianza y lealtad de los usuarios.

Una línea de investigación futura podría enfocarse en explorar cómo la implementación de tecnologías emergentes, como la inteligencia artificial y el blockchain, puede mejorar la ciberseguridad y la protección de datos en las plataformas de comercio electrónico.

## *REFERENCIAS BIBLIOGRÁFICAS*


Bernal, C. (2010). Metodología de la investigación. Pearson Educación de Colombia Ltda.

Docusign Inc. (2023). Confianza del cliente: ¿Cómo ganarla y mantenerla? https://www.docusign.com/es-mx/blog/confianza-del-cliente

Ecuador. Ministerio de Telecomunicaciones. (2022). Diagnóstico de las capacidades de ciberseguridad Ecuador. https://www.telecomunicaciones.gob.ec/wp-content/uploads/2023/05/DIAGNO%CC%81STICO-DE-LAS-CAPACIDADES-DE-CIBERSEGURIDAD-Ecuador-Diciembre-2022_compressed.pdf

Gordillo, A. (2024). Estrategias de ciberseguridad para Mipymes del sector terciario. ***European Public & Social Innovation Review,*** 9, 1-19. https://doi.org/10.31637/epsir-2024-293

Gracy, M. (2024). Top Cybersecurity Challenges Facing Organizations Today. https://sprinto.com/blog/challenges-of-cyber-security/

Hernández Sampier, R., & Mendoza, C. (2018). Metodología de la investigación: Las rutas cuantitativa, cualitativa y mixta. McGraw-Hill Interamericana Editores, S.A. de C.V.

Kashyap, A. K., & Chaudhary, M. (2023). Cyber security laws and safety in e-commerce in India. ***Law and Safety, 89***(2), 207-216. https://pb.univd.edu.ua/index.php/PB/article/view/740

Kumar, H. (2024). 17 Tips to Build Online Trust for Your Business. https://www.linkedin.com/pulse/17-tips-build-online-trust-your-business-hataish-kumar-ilivf/

Medina Herrera, M. A., Erazo Álvarez, J. C., & Cordero Guzmán, D. M. (2024). El impacto de la inteligencia artificial en la personalización de la experiencia del cliente en el e-commerce. ***Universidad Y Sociedad, 16***(4), 49–53. https://rus.ucf.edu.cu/index.php/rus/article/view/4563

Meléndez, E., & Abrego, D. (2021). El papel de la confianza en la intención de uso del comercio electrónico. ***Revista Ibérica de sistemas y tecnologías de información,*** (42), 30-45. https://doi.org/10.21640/ns.v10i21.1611

Merchán, J. (2024). Fortaleciendo la Ciberseguridad con Estrategias proactivas e innovadoras. https://connect.cedia.edu.ec/fortaleciendo-la-ciberseguridad-con-estrategias-proactivas-e-innovadoras/

Narciso, D. (2024). How to Build Trust in eCommerce for Lasting Success. https://debutify.com/blog/how-to-build-trust-in-ecommerce

Peralta, M., & Aguilar, D. (2021). La ciberseguridad y su concepción en las Pymes de Cuenca, Ecuador. ***Contabilidad y Auditoría, 53***(27). https://rest-dspace.ucuenca.edu.ec/server/api/core/bitstreams/7fd596cb-b5d4-4b3c-8057-fe058c4afb96/content

Pimienta, J., & De la Orden, A. (2017). Metodología de la Investigación. Pearson Educación de México.

Rueda, H. (2020). Aplicabilidad del manual de Tallin en la legislación ecuatoriana como respuesta a transgresiones de ciberseguridad. (Tesis de maestría). Universidad Israel.

S2 Grupo. (2024). **Ciberseguridad para pymes: cómo puede beneficiar a tu negocio.** https://s2grupo.es/ciberseguridad-para-pymes-como-puede-beneficiar-a-tu-negocio/