Fecha de presentación: abril, 2024, **Fecha de Aceptación**: mayo, 2024, **Fecha de publicación**: julio, 2024

25

DESARROLLO DE COMPETENCIAS EN SEGURIDAD DE LA INFORMACIÓN Y PROTECCIÓN DE DATOS EN EL COMERCIO ELECTRÓNICO

DEVELOPMENT OF COMPETENCIES IN INFORMATION SECURITY AND DATA PROTECTION IN E-COMMERCE

María Laíz Calderón Peñafiel[1*]
E-mail: maria.calderon.43@est.ucacue.edu.ec
ORCID: https://orcid.org/0009-0008-5677-4466
Diego Marcelo Cordero Guzmán[1]
E-mail: dcordero@ucacue.edu.ec
ORCID: https://orcid.org/0000-0003-2138-2522
Jose Alberto Rivera Costales[1]
E-mail: jriverac@ucacue.edu.ec
ORCID: https://orcid.org/0000-0001-9965-081X
*Autor para correspondencia
[1]Universidad Católica de Cuenca. Ecuador.

Cita sugerida (APA, séptima edición)

Calderón Peñafiel, M. L., Cordero Guzmán, D. M., y Rivera Costales, J. A., (2024). Desarrollo de competencias en seguridad de la información y protección de datos en el comercio electrónico. ***Revista Conrado, 20***(99), 249-259.

RESUMEN

El crecimiento del comercio electrónico ha traído consigo desafíos considerables, entre ellos, la preocupación por la seguridad en las transacciones en línea. El estudio tiene como objetivo desarrollar competencias sobre la protección de datos. Se empleó una metodología mixta, combinando enfoques cualitativos y cuantitativos, así como los métodos inductivo-deductivo, analítico-sintético e histórico. Los resultados destacaron la importancia del muestreo estratificado para representar las diversas realidades de la ciudad. Se identificaron preocupaciones sobre la falta de transparencia en el manejo de datos por parte de las empresas, así como una percepción generalizada de insatisfacción con las medidas de seguridad. Además, se evidenció una falta de conocimiento sobre regulaciones de protección de datos. Es importante enfatizar en la necesidad de mejorar la transparencia, la comunicación y la educación por parte de las empresas para garantizar un entorno seguro y confiable en el comercio electrónico.

Palabras clave:

Privacidad de los datos, digitalización, consumidor, tratamiento de dato, competencia digital.

ABSTRACT

The growth of e-commerce has brought with it considerable challenges, including concerns about the security of online transactions. The study aims to develop competencies on data protection. A mixed methodology was employed, combining qualitative and quantitative approaches, as well as inductive-deductive, analytical-synthetic and historical methods. The results highlighted the importance of stratified sampling to represent the diverse realities of the city. Concerns were identified about the lack of transparency in data management by the companies, as well as a generalized perception of dissatisfaction with security measures. In addition, a lack of knowledge about data protection regulations was evident. It is important to emphasize the need to improve transparency, communication and education on the part of companies to ensure a secure and trustworthy e-commerce environment.

Keywords:

Data privacy, digitization, consumer, data processing, digital competence.

INTRODUCCIÓN

El desarrollo de competencias en seguridad de la información y protección de datos en el comercio electrónico se ha vuelto indispensable dada la creciente relevancia de esta modalidad comercial a nivel global. Especialmente en el contexto posterior a la pandemia de COVID-19, el comercio electrónico se ha consolidado como un pilar fundamental para las empresas. Durante este periodo, Internet ha emergido como el principal canal para mantener los ingresos de numerosas empresas, convirtiéndose en el medio predominante a través del cual los consumidores acceden a productos que no están disponibles en las tiendas físicas. En este sentido, el desarrollo de competencias en seguridad de la información y protección de datos se vuelve crucial para garantizar la confianza de los consumidores en las transacciones en línea.

Los profesionales y empresas que participan en el comercio electrónico deben estar equipados con las habilidades necesarias para proteger los datos sensibles de los clientes y asegurar la integridad de las transacciones en un entorno digital cada vez más complejo y desafiante. Esto incluye el conocimiento de las regulaciones pertinentes, la implementación de medidas de seguridad efectivas y la promoción de la transparencia en el manejo de datos. Sin embargo, este aumento en la actividad del comercio electrónico también ha traído consigo desafíos significativos en términos de seguridad de la información y protección de datos. Con la proliferación de transacciones en línea, la necesidad de desarrollar competencias sólidas en estos aspectos se vuelve crucial. Las empresas y los profesionales involucrados en el comercio electrónico deben estar capacitados para garantizar la seguridad de los datos de los clientes, prevenir el fraude cibernético y cumplir con las regulaciones de privacidad vigentes. Esta capacitación no solo es necesaria para proteger la información confidencial de los usuarios, sino también para mantener la confianza en el comercio electrónico como un medio seguro y confiable de realizar transacciones (Orús, 2023).

El comercio se adapta constantemente a los cambios generacionales y avances tecnológicos. La globalización y la expansión de Internet han dado lugar al surgimiento del comercio electrónico, permitiendo que una gran parte de la población mundial acceda a la tecnología y encuentre información, productos y servicios adaptados a sus necesidades e intereses. Empresas líderes en el ámbito tecnológico, como Amazon, Apple, Google y otras, han dejado una huella relevante en la economía a través de esta nueva forma de comercio.

En el Ecuador, el comercio electrónico se concentra principalmente en las principales ciudades del país, especialmente en Quito, Guayaquil y Cuenca, según datos del Instituto Ecuatoriano de Estadísticas y Censos (INEC). Estas ciudades representan el 51% del comercio electrónico en Ecuador, siendo las prendas de vestir y el calzado los productos más demandados, abarcando el 33% de las compras en línea. Aunque el porcentaje de la población nacional que realiza compras en línea es relativamente bajo, apenas el 0.34%, la tendencia sugiere un crecimiento constante en esta forma de consumo (Chiriguayo, 2015).

En consecuencia, el desarrollo del comercio electrónico también plantea desafíos importantes, entre ellos, la preocupación sobre la seguridad de las transacciones en línea. A diferencia del comercio tradicional, donde las transacciones se realizan de forma segura en persona o mediante métodos tradicionales, en el comercio electrónico la interacción entre compradores y vendedores se realiza a través de Internet. Una plataforma abierta no puede garantizar una comunicación segura sin las medidas de seguridad adecuadas.

Otro de los principales desafíos es la divulgación de información personal y confidencial de los clientes, como números de tarjetas de crédito, en un entorno completamente abierto como Internet. Además, no se sabe cómo obtener un recibo que permita reclamaciones posteriores tanto contra el comprador como contra el vendedor si, tras completar la transacción, una de las partes decide que la otra causó el daño (Heredia y Villarreal, 2022).

Para abordar estos desafíos, existen diversos protocolos electrónicos diseñados para garantizar la seguridad en las transacciones en línea, como el SET (Secure Electronic Transaction) o el SSL (Secure Sockets Layer). Sin embargo, ninguno de ellos ofrece una seguridad absoluta en la actualidad, dejando tanto al comprador como al vendedor susceptible a posibles fraudes. Es crucial reconocer que, en el comercio electrónico, la seguridad no es simplemente una opción adicional, sino un componente fundamental para la viabilidad y el éxito de cualquier proyecto de compra o venta en línea (Maldonado, 2017).

Ante la creciente adopción del comercio electrónico en la ciudad de Cuenca, combinada con los riesgos inherentes a la exposición de datos personales y financieros en línea, surge el problema de investigación ¿cómo mejorar la seguridad de la información del comercio electrónico de la ciudad de Cuenca?, para ello, se plantea el objetivo desarrollar competencias sobre seguridad del comercio electrónico de la ciudad de Cuenca que permita proteger sus datos.

El avance de las nuevas tecnologías ha suscitado una clara preocupación en cuanto a la privacidad de los ciudadanos, así como de los consumidores y usuarios en particular. Las telecomunicaciones, al facilitar la recopilación, análisis, almacenamiento y uso de información por parte de los proveedores, han contribuido a esta preocupación. Este aumento en la disponibilidad y utilización de datos ha generado un nuevo desafío en términos de manejo y respeto de los datos personales, requiriendo la implementación de mecanismos de protección en todas las etapas, desde la recopilación inicial hasta su posible transferencia a terceros, independientemente del medio de almacenamiento. La creciente disponibilidad y uso de datos ha llevado a la búsqueda de formas de proteger la privacidad y seguridad de las personas en un entorno cada vez más digitalizado (Vega, 2013).

En este escenario, el consentimiento emerge como una herramienta esencial que otorga a los usuarios el control sobre el tratamiento de sus datos personales. Se considera que el consentimiento es una base legal adecuada únicamente si se garantiza al individuo un auténtico control y capacidad de elección en relación con la aceptación o rechazo de las condiciones propuestas, sin sufrir consecuencias adversas por su negativa. Por consiguiente, es deber del encargado del tratamiento de datos evaluar si el consentimiento obtenido satisface todos los requisitos legales para ser considerado válido. En última instancia, el consentimiento se percibe como un elemento fundamental que permite a los individuos decidir si desean que sus datos personales sean procesados o no, reafirmando así su derecho a la privacidad y autonomía en el entorno digital (Andrés, 2019).

El desarrollo del comercio electrónico en todo el mundo ha llevado a la adopción de leyes y reglamentos que regulan la gestión y protección de datos personales. Por ejemplo, la Unión Europea ha adoptado el Reglamento General de Protección de Datos (GDPR), que establece reglas claras sobre la recopilación, el procesamiento y la divulgación de datos personales, brindando a los ciudadanos un mayor control y seguridad sobre sus datos personales en línea. Estas leyes, además de brindar a los usuarios un mayor control y seguridad sobre sus datos personales en el mundo digital, también restringen la transferencia de datos personales a otros países (MacColl, 2019).

Por lo tanto, las organizaciones y los proveedores de servicios en línea deben considerar la importancia de asumir la responsabilidad principal de proteger la privacidad de los datos personales de los usuarios de acuerdo con este derecho básico. De igual forma, se enfatiza la importancia de las obligaciones estatales a nivel internacional a través de la ratificación de acuerdos y tratados multilaterales para proteger los intereses y derechos de los usuarios y consumidores en el comercio electrónico a escala global (Ordóñez, 2010).

En cuanto a la normativa europea, Ecuador cuenta con organismos como el Consejo Nacional de Telecomunicaciones (CONATEL) que se han comprometido a impulsar regulaciones para garantizar la seguridad de la información y la privacidad de los datos en el comercio electrónico. Es muy importante que estas regulaciones no sean vistas como barreras a las transacciones electrónicas sino como medidas para proteger los intereses y derechos de los usuarios y consumidores de Internet. En este sentido, son necesarios compromisos mediante la ratificación de acuerdos y tratados multilaterales para garantizar la protección integral de los datos personales en el entorno del comercio electrónico a escala global.

Ahora bien, al hablar de la seguridad de la información, su propósito principal es asegurar la confidencialidad y la integridad de la información, evitando operaciones no autorizadas como la publicación, modificación o eliminación de datos. Según la Norma ISO 27001, la seguridad de la información se define como la protección de la confidencialidad, integridad y disponibilidad de los datos, pudiendo incluir también otras características como autenticidad, responsabilidad, fiabilidad y no repudio. En última instancia, su objetivo es garantizar un proceso sin peligro ni riesgo de daño para la información (Pozo et al., 2023).

La seguridad de la información se sustenta en tres principios esenciales: confidencialidad, integridad y disponibilidad, comúnmente referidos como la tríada de CIA. Este modelo ha sido ampliamente reconocido y empleado durante más de veinte años, ofreciendo un sólido marco conceptual para analizar y discutir aspectos vinculados a la seguridad. Se enfoca principalmente en salvaguardar la integridad de los datos, aunque no excluye otros aspectos relevantes (Parada et al., 2018).

La confidencialidad, en particular, se centra en prevenir el acceso no autorizado a los datos. Puede aplicarse en diversos niveles del proceso. Por otro lado, la integridad se refiere a prevenir modificaciones no autorizadas o no deseadas en nuestros datos, lo que incluye tanto cambios indeseados como reversión de cambios autorizados. Y como tercer componente tenemos a la disponibilidad, que se relaciona con acceder a nuestros datos cuando lo necesitamos, evitando interrupciones en la cadena de comunicaciones que puedan dificultar dicho acceso, tales como fallos de energía, problemas de sistemas, ataques a la red o compromisos de sistemas. Los ataques

de denegación de servicio (DoS) son una de las causas comunes de tales problemas (Vega, 2021).

El desarrollo de competencias en seguridad de la información y protección de datos se vuelve aún más crucial cuando consideramos que, a pesar de los esfuerzos por establecer estándares sólidos, los sistemas de comercio electrónico continúan siendo altamente vulnerables a diversas amenazas. Esta realidad resalta la importancia de adoptar un enfoque proactivo en la gestión de riesgos de seguridad y mejorar constantemente las medidas de ciberseguridad para proteger la información digital. En respuesta a esta necesidad creciente, el mercado ofrece una amplia gama de herramientas y gestores especializados en seguridad de la información, diseñados específicamente para abordar las necesidades del comercio electrónico y mitigar vulnerabilidades de manera efectiva.

El desarrollo de competencias en el uso de estas herramientas y en la implementación de prácticas sólidas de seguridad cibernética se vuelve esencial para salvaguardar la integridad y la confidencialidad de los datos en el entorno digital del comercio electrónico. Además, la formación continua y la actualización de conocimientos son aspectos fundamentales para mantenerse al día con las nuevas amenazas y tecnologías emergentes en el campo de la seguridad de la información (De La Cruz et al., 2023). Estas soluciones son esenciales para mantener la integridad y seguridad de los datos de los usuarios y consumidores en un entorno cada vez más digital.

MATERIALES Y MÉTODOS

El enfoque de metodología mixta, cualitativa y cuantitativa adoptado en este estudio permitió una exploración exhaustiva y rigurosa del tema bajo investigación. La integración de métodos cualitativos y cuantitativos ofreció una perspectiva multidimensional que enriqueció la comprensión del tema. Mientras que los métodos cualitativos facilitaron la exploración en profundidad de las experiencias y percepciones de los participantes, los enfoques cuantitativos proporcionaron datos numéricos y estadísticos que permitieron probar hipótesis con base en la medición numérica y análisis de tendencias. Esta combinación sinérgica de enfoques no solo enriqueció la investigación, sino que también mejoró su validez y fiabilidad al abordar a cada método de manera complementaria (Hernández et al., 2014). Se logró una comprensión más amplia y holística del tema investigado, lo que enriqueció el conocimiento en este campo y promovió un avance significativo en la comprensión del tema.

En la presente investigación, fue importante considerar distintos métodos que permitieran abordar el tema de estudio desde diferentes perspectivas. Desde una óptica macro, se empleó el método deductivo, partiendo de teorías generales para luego contrastarlas con la realidad específica objeto de estudio. Por otro lado, a nivel meso, se utilizó el método analítico-sintético, descomponiendo el problema en elementos más simples para comprender su funcionamiento y luego sintetizar estos hallazgos en una visión global. A nivel micro, se recurrió al método inductivo, observando patrones y fenómenos particulares para derivar conclusiones generales. Además, se integró el análisis histórico para comprender cómo ha evolucionado el tema de investigación a lo largo del tiempo, brindando perspectivas valiosas sobre su contexto y desarrollo.

El diseño de la investigación adoptado fue de carácter no experimental, lo que implicó observar y registrar fenómenos tal como se presentaron en su entorno natural (Arispe et al., 2020). Esta elección metodológica se fundamentó en la necesidad de comprender fenómenos tal como se manifestaron en la realidad, sin intervenciones que pudieran alterar su naturaleza, lo que contribuyó a la validez externa de los resultados obtenidos.

En cuanto al tipo de investigación aplicada, se centró en la resolución de problemas prácticos y la generación de conocimiento con aplicaciones directas en la realidad (Vargas, 2009). La investigación se centró en establecer una colaboración estrecha con los principales actores del ámbito de estudio, con el propósito de recopilar información crucial sobre la protección de datos de los usuarios del comercio electrónico en la ciudad de Cuenca. Para lograr este cometido, se desarrolló un cuestionario como herramienta de evaluación, garantizando así la pertinencia y utilidad de los resultados para abordar desafíos específicos en este campo.

RESULTADOS Y DISCUSIÓN

El estudio sobre los desafíos de seguridad de la información y protección de datos en el comercio electrónico en la ciudad de Cuenca, Ecuador, ha destacado la importancia del muestreo estratificado como herramienta esencial para comprender este análisis en relación al avance tecnológico que hoy día se enfrenta. Al dividir a la población en subgrupos homogéneos según criterios geográficos, este enfoque permite una representación precisa y equilibrada de la diversa realidad de la ciudad. Esto es importante en un entorno donde los requisitos de seguridad de la información y las necesidades de protección de datos varían significativamente entre diferentes regiones y segmentos de población.

La aplicación del muestreo estratificado a una muestra de 98 usuarios ha proporcionado una visión amplia y

detallada de las experiencias y opiniones de los usuarios de comercio electrónico en Cuenca. Cada estrato geográfico ha aportado información valiosa, enriqueciendo la comprensión de los desafíos de seguridad en el comercio electrónico en la ciudad.

A partir de este análisis, se han identificado tendencias y problemas específicos en diversos aspectos del comercio electrónico. Esto proporciona una base sólida para desarrollar estrategias y políticas para mejorar la seguridad del comercio electrónico y proteger los datos personales de los usuarios. Además, enfatiza la necesidad de un enfoque adaptado a las diversas realidades geográficas y demográficas de las ciudades, al tiempo que reconoce que las soluciones efectivas deben abordar los desafíos específicos de cada ciudad y la composición de la población en su propio contexto.

El siguiente estudio se centra en analizar las interrelaciones entre diversas variables clave. La Tabla 1 que se presenta a continuación ofrece una visión detallada de la correlación entre estas variables, lo que proporcionará una comprensión más profunda de su impacto y relación dentro del contexto de la investigación.

Tabla 1. Correlación entre variables de investigación.

	Consentimiento de datos en comercio electrónico			
Uso de datos	A veces	Nunca	Siempre	Total
A veces	30	3	6	39
Nunca	32	19	3	54
Siempre	2	2	1	5
Total	64	24	10	98

Fuente: Elaboración de autores

La tabla presenta los coeficientes de correlación entre las variables independiente y dependientes investigadas en el estudio, proporcionando una visión más clara de lo analizado.

Los resultados de la correlación entre las variables de investigación indican que la mayoría de los participantes no perciben una solicitud clara de consentimiento por parte de las empresas de comercio electrónico antes de la recopilación y procesamiento de sus datos personales. Este resultado destaca la necesidad de una mayor transparencia en las prácticas de privacidad en línea. Además, la transparencia en cuanto al uso de datos con fines publicitarios también es cuestionada, solo una minoría muy pequeña (5%) siente que estas empresas siempre les informan de manera transparente.

Estos hallazgos sugieren, una falta de claridad y transparencia por parte de las empresas de comercio electrónico en cuanto a la recopilación y el uso de datos personales de los usuarios. Por lo tanto, los resultados destacan la necesidad de mejorar las prácticas de consentimiento y transparencia en este sector para aumentar la confianza del consumidor y cumplir con las regulaciones de privacidad.

Por otra parte, se presenta la Tabla 2, la cual ofrece una comparación detallada de las proporciones relacionadas con la variable de protección de datos en comparación con la seguridad de la información. Este análisis proporciona una visión más clara de la interacción entre estas dos variables clave en el contexto de nuestro estudio.

Tabla 2. Proporciones contrastadas de la variable protección de datos.

Variable	Nivel	Recuentos	Total	Proporción	p
Satisfacción con las medidas de seguridad y protección de datos	Muy satisfecho	2	98	0.020	< .001
	Nada satisfecho	9	98	0.092	< .001
	Poco satisfecho	52	98	0.531	0.614
	Satisfecho	35	98	0.357	0.006

Fuente: Elaboración de autores

Proporciones contrastadas en relación al valor: 0.5 de la satisfacción con las medidas de seguridad en el comercio electrónico.

Los resultados indican que la gran mayoría de los encuestados no están completamente conformes con las medidas de seguridad y protección de datos proporcionadas por las empresas de comercio electrónico que utilizan, ya que solo el 2% se muestra muy complacido. Estos datos sugieren una percepción generalizada de insatisfacción con las medidas de seguridad y protección de datos en el ámbito del comercio electrónico. La notable disparidad entre aquellos que están poco satisfechos y aquellos que están satisfechos subraya la necesidad de mejorar las políticas y prácticas de protección de datos por parte de las empresas para asegurar la confianza y satisfacción del cliente.

Ahora bien, en la Tabla 3 se muestra cómo las empresas solicitan de manera clara y transparente el consentimiento de datos antes de recopilar y procesar información para diferentes fines.

Tabla 3. Claridad en la solicitud de consentimiento para el manejo de datos personales.

Transparencia en la recopilación y procesamiento de datos personales	Frecuencia	Porcentaje	Porcentaje Válido	Porcentaje Acumulado
Clara	25	25.510	25.510	25.510
Muy clara	2	2.041	2.041	27.551
Nada clara	13	13.265	13.265	40.816
Poco clara	58	59.184	59.184	100.000
Total	98	100.000		

Fuente: Elaboración de autores

La tabla presenta la proporción de encuestados que señalaron la influencia de la variable de protección de datos en el ámbito del comercio electrónico, ofreciendo una perspectiva sobre la percepción de la importancia de la protección de datos entre los participantes.

Solo una minoría relativamente pequeña percibe claridad en el proceso de solicitud de consentimiento, con el 25.51% considerándola clara y solo el 2.04% la calificando como muy clara. Estos hallazgos subrayan la urgencia de mejorar la transparencia y claridad en las prácticas de solicitud de consentimiento por parte de las empresas de comercio electrónico, lo que podría contribuir a incrementar la confianza y satisfacción del consumidor.

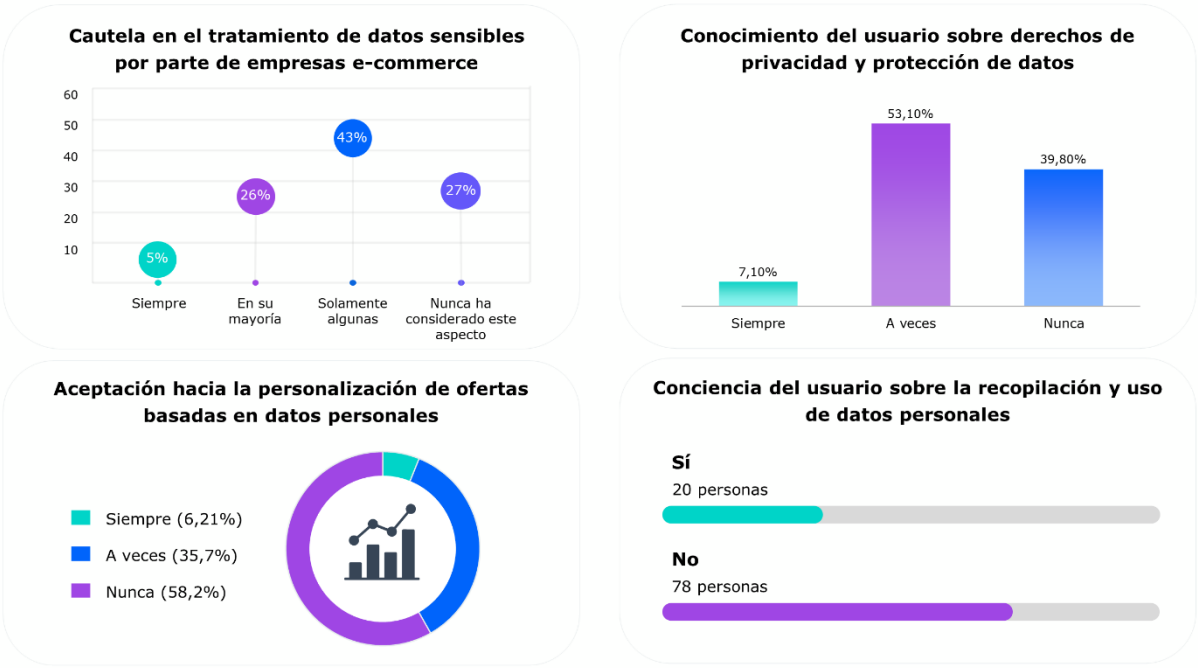
Dentro de este marco, la Figura 1 ofrece un análisis detallado de algunas variables adicionales que proporcionarán una comprensión más completa de cómo los usuarios perciben el comercio electrónico y el manejo de datos, incluida la seguridad de la información proporcionada en este entorno.

El análisis de chi-cuadrado revela una asociación significativa entre las variables dependiente mejoramiento de la seguridad de la información del comercio electrónico de la ciudad de Cuenca e independiente desarrollo competencias sobre seguridad del comercio electrónico, con un valor de chi-cuadrado (X^2) de 4.107 y un nivel de significancia (p) de 0.0250. Esto indica que hay una relación entre el desarrollo de competencias sobre seguridad del comercio electrónico y el esfuerzo por mejorar la seguridad de la información en el comercio electrónico de Cuenca.

El valor de chi-cuadrado sugiere que la discrepancia entre las frecuencias observadas y esperadas no es resultado del azar, sino que hay una asociación real entre las variables. Además, el p-valor inferior al nivel de significancia comúnmente utilizado de 0.05 indica que esta asociación es estadísticamente significativa.

Con un tamaño de muestra de 98, estos resultados sugieren que el desarrollo de competencias sobre seguridad del comercio electrónico podría ser un factor importante para mejorar la seguridad de la información en el comercio electrónico de Cuenca.

Fig. 1. Dashboard – Resultados del uso y tratamiento de datos en diferentes aspectos del comercio electrónico.



Fuente: Elaboración de autores

El análisis de los resultados destaca la preocupante falta de transparencia en el manejo de datos personales por parte de las plataformas de comercio electrónico, lo que subraya la importancia del desarrollo de competencias en seguridad de la información y protección de datos en este contexto. Con un abrumador 79.6% de los encuestados expresando su falta de información sobre cómo se recopilan y utilizan sus datos personales en estos servicios, se evidencia una notable discrepancia entre las expectativas de los usuarios y la realidad de la gestión de datos en línea. Esta discrepancia resalta la necesidad de que los profesionales del comercio electrónico adquieran competencias en seguridad de la información para garantizar una gestión transparente y ética de los datos de los usuarios.

Además, la falta de conciencia sobre la importancia de la seguridad de los datos es preocupante, ya que una proporción considerable (26.5%) de los encuestados nunca ha considerado este aspecto. Esto subraya la necesidad de desarrollar competencias en seguridad de la información entre los usuarios para que puedan comprender los riesgos asociados y tomar medidas preventivas.

La falta de conocimiento sobre las leyes y regulaciones de protección de datos, evidenciada por el 74.5% de los encuestados que no están familiarizados con estas normativas, pone de relieve la importancia del desarrollo de competencias legales en el ámbito del comercio electrónico. Los profesionales deben comprender y cumplir con las regulaciones de protección de datos para garantizar el cumplimiento legal y la protección de la privacidad de los usuarios.

La falta de comunicación sobre los derechos del consumidor en términos de privacidad y protección de datos resalta la necesidad de que las empresas de comercio electrónico desarrollen competencias en comunicación y educación para informar adecuadamente a los usuarios sobre sus derechos y cómo se protegen sus datos.

Los resultados de investigaciones realizadas por diversos autores ofrecen una visión diversa sobre el impacto de la seguridad y la confianza en el comercio electrónico. Estos estudios abordan aspectos que van desde la percepción del consumidor hasta los marcos legales y las prácticas empresariales. En este contexto, se exploran no solo los elementos técnicos que contribuyen a la seguridad en línea, sino también la importancia de la transparencia en la recolección y procesamiento de datos personales, así como la necesidad de cumplir con regulaciones específicas en materia de protección de datos. Esta variedad de enfoques refleja la complejidad inherente para asegurar un entorno digital seguro y confiable para los usuarios del comercio electrónico.

Por lo tanto, según la investigación realizada por Salas-Rubio y Ábrego-Almazán (2024), se proporciona un análisis detallado sobre el papel de la seguridad y la confianza en el proceso de aceptación y utilización del comercio electrónico. Se destaca que la seguridad tiene un impacto positivo y significativo en la generación de confianza en las compras en línea. Esto implica que los usuarios necesitan percibir un entorno seguro en las plataformas en línea para sentirse cómodos realizando transacciones por Internet. Así pues, la seguridad no solo representa un requisito técnico, sino que también se posiciona como un elemento clave para fomentar la confianza del consumidor en el comercio electrónico.

Además, se encontró una relación positiva entre la confianza en el vendedor en línea y la actitud del consumidor hacia la compra en línea. Cuando los vendedores proporcionan herramientas de seguridad de datos y cumplen con las expectativas del cliente, se fortalece la confianza, lo que a su vez aumenta su intención de realizar compras en línea. Esta relación subraya la importancia de que las empresas implementen medidas de seguridad sólidas y transparentes para fomentar la confianza del consumidor y promover el uso continuo del comercio electrónico.

De igual manera se encontró que la actitud del usuario se destaca como una variable secundaria con una mayor capacidad predictiva e impacto en comparación con otras variables dependientes. Esto indica que la actitud del consumidor hacia el comercio electrónico juega un papel esencial en su conducta de compra en línea. Por consiguiente, al desarrollar estrategias de comercio electrónico, es esencial tener en cuenta y abordar las actitudes y percepciones de los consumidores hacia la seguridad y la confianza en línea.

Por otra parte, los hallazgos del estudio realizado por Bilbao (2022), acerca los desafíos relacionados con la seguridad de la información y la protección de datos en el entorno del comercio electrónico, identifican varios aspectos cruciales que reflejan las inquietudes sobre el riesgo moral y los incentivos desalineados en el ámbito de la ciberseguridad.

Se evidencia una clara asimetría de información entre los usuarios y las empresas de comercio electrónico. Los datos muestran que la mayoría de los encuestados no perciben que las empresas les soliciten su consentimiento de manera clara antes de recopilar y procesar sus datos personales. Esta falta de transparencia y claridad puede llevar a situaciones de riesgo moral, donde los usuarios se ven en una posición de desventaja al no comprender completamente cómo se utilizan sus datos.

Así mismo, se destaca la importancia crucial de establecer estándares claros para la presentación de información sobre seguridad y protección de datos en el ámbito del comercio electrónico, con el objetivo de evitar confusiones y garantizar la transparencia. La amplia insatisfacción con las medidas actuales de seguridad y protección de datos proporciona una señal clara de la necesidad urgente de reformar y fortalecer las políticas y prácticas en esta área. Este llamado de atención subraya la importancia crítica de abordar las deficiencias existentes y fomentar una mayor transparencia y responsabilidad en la gestión de la seguridad y la protección de datos en el comercio electrónico.

Se observa que las empresas tienden a priorizar la funcionalidad sobre la seguridad en el desarrollo de aplicaciones y servicios de comercio electrónico. Esta tendencia puede resultar en productos inseguros para los usuarios, lo que nuevamente refuerza la importancia de alinear los incentivos para garantizar la seguridad de los sistemas y datos.

Los hallazgos también señalan una carencia de comprensión sobre la relevancia de la seguridad y las regulaciones de protección de datos entre los usuarios. Esta falta de conciencia puede poner a los usuarios en riesgo en términos de privacidad y seguridad, enfatizando la importancia de la educación y la sensibilización sobre estos asuntos.

En última instancia, la investigación resalta que resolver los desafíos relacionados con la seguridad de la información y datos en el comercio electrónico no se limita únicamente a cuestiones técnicas, sino que también involucra aspectos humanos. Las elecciones y comportamientos individuales impactan en la seguridad de los sistemas, por lo que es esencial tener en cuenta tanto los aspectos técnicos como los humanos en la salvaguarda de la información y la privacidad en el entorno digital.

En base a los desafíos identificados en la seguridad de la información y protección de datos, el estudio realizado por Benussi (2020), destaca resultados alarmantes que coinciden con las preocupaciones planteadas en el ámbito chileno. Tanto en Chile como en otros lugares, hay una preocupación creciente sobre la seguridad de los datos personales debido a la frecuente exposición a violaciones en los sistemas informáticos, lo que afecta la confianza de los usuarios al momento de hacer uso del comercio electrónico.

La era de la información ha provocado una transformación notable en diversos ámbitos, elevando la relevancia de implementar medidas de seguridad tanto a nivel institucional como personal en el manejo de datos. Este

cambio es notorio incluso, en la investigación realizada en la ciudad de Cuenca, donde se destaca la necesidad imperativa de fortalecer las políticas y procedimientos de protección de datos en el ámbito del comercio electrónico. Mejorar estos aspectos no solo es crucial para garantizar la confianza de los consumidores, sino también para cumplir con las regulaciones de privacidad vigentes.

La importancia del manejo extensivo de datos personales y el incremento de incidentes de seguridad asociados resaltan la necesidad de promover una regulación más efectiva de las responsabilidades de seguridad de los datos personales para salvaguardar los derechos fundamentales. Este aspecto resulta crucial tanto en el entorno chileno como en el ecuatoriano, enfatizando la importancia de adoptar medidas de seguridad adecuadas que tengan en cuenta factores como el nivel actual de la tecnología disponible, los costos de implementación y la sensibilidad de los datos manipulados.

En el ámbito internacional, la interconexión entre las salvaguardas esenciales ligadas a la preservación de la privacidad y el resguardo de la seguridad personal ha incidido en la formulación de compromisos legales sobre la seguridad en el manejo de datos personales en jurisdicciones locales. Este patrón reitera la significancia de establecer y acatar obligaciones de seguridad eficaces en ambas esferas, reconociendo la urgencia de realizar investigaciones más exhaustivas y establecer regulaciones pertinentes.

En ambos contextos, tanto en Chile como en Cuenca, Ecuador, los hallazgos subrayan la vital importancia de instaurar y seguir rigurosamente obligaciones de seguridad eficaces en el manejo de datos personales, con el propósito de resguardar la privacidad y los derechos esenciales de las personas. Esta inquietud compartida pone de relieve la urgencia de tomar medidas concretas para fortalecer la seguridad de la información y la protección de datos, tanto en el comercio electrónico como en otros aspectos de la era digital.

Por lo tanto, el manejo cuidadoso y efectivo de la información de datos personales, se extiende a una visión más amplia donde según la investigación elaborada por Mardones et al. (2023), proporcionan un análisis sobre el uso de sistemas de información en el comercio electrónico para la satisfacción del cliente, contrastando con el crecimiento significativo en la producción científica en este campo en los últimos años. Este aumento en la productividad científica refleja tanto los avances como los desafíos en la implementación de sistemas de información en empresas de comercio electrónico que manejen estándares de seguridad. Se destaca un crecimiento lineal en la producción científica sobre sistemas de información en el comercio electrónico desde 1998 hasta 2022, con un notable incremento del 98.5% en el número de artículos publicados en este tema.

Este análisis proporciona una visión general de los principales contribuyentes en el ámbito de la investigación científica sobre sistemas de información en el comercio electrónico. Al contrastar estos resultados con los hallazgos específicos obtenidos de la investigación sobre seguridad de la información y protección de datos en el comercio electrónico en la ciudad de Cuenca, Ecuador, emerge una situación compleja. Aunque el aumento en la producción científica sugiere un interés continuo y creciente en mejorar la experiencia del cliente en el comercio electrónico mediante el desarrollo de sistemas de información, los resultados específicos de la investigación en Cuenca evidencian desafíos notables en términos de transparencia, claridad en la solicitud de consentimiento y satisfacción del cliente con las medidas de seguridad brindadas.

Estos hallazgos subrayan la necesidad de integrar avances teóricos y prácticos en la implementación de sistemas de información en el comercio electrónico. Si bien existe un crecimiento en la producción científica y una identificación de líderes en el campo, es esencial abordar las preocupaciones específicas de los usuarios y las realidades locales, como se evidencia en la investigación realizada en Cuenca. Además, la brecha entre el conocimiento académico y las prácticas en el terreno subraya la importancia de la investigación aplicada y la colaboración entre académicos y profesionales en el desarrollo de soluciones efectivas y adaptadas a contextos específicos.

Si bien los avances en sistemas de información para el comercio electrónico son evidentes a nivel global, la investigación específica resalta la necesidad de abordar desafíos locales y preocupaciones de los usuarios para mejorar la eficacia y la confianza en estos sistemas.

Otra perspectiva sobre los temas investigados se encuentra en el estudio realizado por Arcos et al. (2023), donde se identifican una serie de inquietudes importantes que coinciden con los principios fundamentales establecidos tanto en la Ley de protección de datos personales en nuestro país como en Colombia. Estas legislaciones establecen directrices para el manejo de datos personales, regulaciones sobre la transferencia internacional de datos o información personal y disposiciones concernientes al tratamiento de datos que pueden llegar a ser sensibles para los usuarios. Sin embargo, es relevante destacar que existen diferencias significativas entre ambas leyes.

Una de las diferencias sobresalientes es la restricción en Colombia del tratamiento de datos sensibles, a diferencia de Ecuador donde se permite cierta flexibilidad al respecto. Estas discrepancias en las regulaciones pueden impactar la forma en que las empresas gestionan la seguridad de información personal y la transparencia en su utilización. Además, las entidades reguladoras designadas para hacer cumplir cada normativa también pueden diferir, lo cual podría influir en la ejecución y el acatamiento de las regulaciones en cada país.

En este sentido, se destaca la necesidad de mejorar la ejecución de las leyes vigentes en ambos países. Se reconoce la escasez de profesionales que tengan conocimientos especializados entre el ámbito legal y el informático, lo que puede complicar la aplicación efectiva de las normativas de protección de datos en cualquier entorno. Es esencial llevar a cabo una evaluación de riesgos adecuada que permita tomar decisiones fundamentadas y asignar los recursos de manera apropiada, dado que la ausencia de este análisis puede dejar a las organizaciones vulnerables a ataques cibernéticos y sufrir pérdidas significativas, tal como lo evidencian los resultados de la presente investigación.

Para atender estas inquietudes, se aluden a regulaciones normalizadas como la ISO 27001, ISO 27002 y la ISO 27003, las cuales brindan pautas para establecer en cualquier entorno digital un Sistema de Gestión de Seguridad de la Información (SGSI) ajustado a las necesidades de cualquier entidad. Estos estándares ofrecen un marco robusto para fortalecer la seguridad cibernética en conformidad con las normativas internacionales.

Además, se presentan recomendaciones clave para las empresas, como identificar claramente el rol de responsable de protección de datos, definir medidas de seguridad básicas, establecer un inventario de actividades de tratamiento y capacitar al personal en normativas y procesos internos. Implementar estas acciones resulta fundamental para reforzar la seguridad y mejorar la credibilidad del comercio electrónico, cerrando así la brecha de falta de conocimiento que muestran los usuarios.

Por consiguiente, la integración de ambas estrategias de investigación, combinando los aspectos relacionados con la seguridad y la confianza en el comercio electrónico, tiene el potencial de impulsar aún más la efectividad y la adopción de este modelo comercial. Al profundizar en la comprensión de cómo la seguridad y la confianza interactúan y se influyen mutuamente, se pueden identificar mejores prácticas y estrategias para fortalecer la experiencia del usuario y fomentar una relación más sólida en las plataformas en línea. Esta sinergia, puede generar un entorno digital más seguro y acogedor, lo que a su vez promueve un mayor compromiso y lealtad por parte de los usuarios, contribuyendo así al crecimiento y la sostenibilidad a largo plazo del comercio electrónico.

CONCLUSIONES

Los hallazgos revelan una falta generalizada de transparencia en el ámbito del comercio electrónico en lo que respecta al manejo de la seguridad de la información y los datos personales de los usuarios. La mayoría de los encuestados perciben que no se solicita su consentimiento de manera clara antes de recopilar y procesar sus datos. Esta situación subraya la importancia de desarrollar competencias sólidas en seguridad de la información y protección de datos en el ámbito del comercio electrónico.

Se observa que la mayoría de los usuarios no están completamente satisfechos con las medidas de seguridad y protección de datos ofrecidas. La brecha entre los usuarios poco satisfechos y los satisfechos subraya la importancia de perfeccionar las políticas y procedimientos de protección de datos con el objetivo de asegurar la confianza y la satisfacción del consumidor en el ámbito del comercio electrónico. Esto resalta la necesidad de formar a los profesionales del comercio electrónico en competencias de seguridad de la información y protección de datos para garantizar la implementación efectiva de medidas de seguridad robustas.

Los resultados muestran una falta significativa de familiaridad entre los usuarios con las leyes y regulaciones de protección de datos. Esta falta de conocimiento puede exponer a los usuarios a riesgos de privacidad y seguridad. Por lo tanto, se necesita una mayor educación y conciencia sobre los derechos del consumidor en términos de privacidad y seguridad informática para abordar esta brecha de conocimiento. Esto subraya la importancia de integrar el desarrollo de competencias en seguridad de la información y protección de datos en los programas educativos y de formación relacionados con el comercio electrónico.

Los hallazgos enfatizan la urgencia de mejorar la transparencia, la comunicación y la educación por parte de las empresas que tienen como giro de negocio el comercio electrónico. Es esencial que los usuarios estén debidamente informados y capacitados en materia de protección de datos para asegurar un entorno de comercio electrónico seguro y confiable. El desarrollo de competencias en seguridad de la información y protección de datos emerge como un componente crítico para abordar los desafíos y garantizar la confianza tanto de los consumidores

como de las empresas en el entorno digital del comercio electrónico.

REFERENCIAS BIBLIOGRÁFICAS

Andrés, G. (2019). ***El consentimiento y el reglamento de protección de datos***. https://www.legaltoday.com/practica-juridica/derecho-publico/proteccion-datos/el-consentimiento-y-el-reglamento-de-proteccion-de-datos-2019-10-04/

Arcos, M., Matute, K., y Fernández, M. (2023). Análisis comparativo de la Ley Orgánica de Protección de Datos Personales del Ecuador con la legislación colombiana desde un enfoque deciberseguridad y delitos informáticos. ***Revista Ibérica de Sistemas e Tecnologias de Información***, 60, 100-114. https://www.proquest.com/openview/d29c2f8f2bdc11ccd4644ff0be3d8b56/1?pq-origsite=gscholar&cbl=1006393

Arispe, C., Yangali, J., Guerrero, M., Lozada, O., Acuña, L., y Arellano, C. (2020). ***La investigación científica.*** Universidad Internacional del Ecuador.

Benussi, C. (2020). Obligaciones de seguridad en el tratamiento de datos personales en Chile: Escenario actual y desafíos regulatorios pendientes. ***Revista Chilena de derecho y tecnología, 9***(1), 231-239. http://dx.doi.org/10.5354/0719-2584.2020.56660

Bilbao, S. (2022). Situaciones de riesgo moral e incentivos desalineados en ciberseguridad. ***Revista Chilena de derecho y tecnología, 11***(1), 107-111. http://dx.doi.org/10.5354/0719-2584.2022.60821

Chiriguayo, S. (2015). Comercio Electrónico: Importancia de la seguridad en las transacciones electrónicas, amenazas y soluciones a implementar. ***Revista Empresarial, ICE-FEE-UCSG, 9***(35). https://editorial.ucsg.edu.ec/ojs-empresarial/index.php/empresarial-ucsg/article/view/15

De La Cruz Rodríguez, G. R., Méndez Fernández, R. A., y Mendoza De Los Santos, A. C. (2023). Seguridad de la información en el comercio electrónico basado en ISO 27001: Una revisión sistemática. ***Innovación Y Software***, ***4***(1), 219-236. https://doi.org/10.48168/innosoft.s11.a79

Heredia, D., & Villarreal, F. (2022). El comercio electrónico y su perspectiva en el mercado. ***ComHumanitas Revista Cientifica de Comunicación, 13***(1), 24-25. https://doi.org/10.31207/rch.v13i1.333

Hernández, R., Fernádez, C., y Baptista, P. (2014). ***Metodología de la investigación***. Mc GRAW-HILL.

MacColl, D. (2019). ¿Qué es RGPD (o GDPR)? https://www.fortra.com/es/blog/que-es-gdpr

Maldonado, J. (2017). Comercio electrónico. Ideas fundamentales. Gestiopolis.https://www.gestiopolis.com/comercio-electronico-ideas-fundamentales/

Mardones, R., Patiño, J., Valencia, A., Londoño, W., Moreno, G., Bermeo, M., y Ore, A. (2023). Tendencias en el uso de sistemas de información en comercio electrónico para la satisfacción del cliente. ***Revista Ibérica de Sistemas e Tecnologias de Información, 59***, 179-190. https://www.proquest.com/openview/68186296ed7437e2db386efc1935ee1f/1?pq-origsite=gscholar&cbl=1006393

Ordóñez, A. L. (2010). Utilización de la firma digital para la protección de datos personales como medio de seguridad en las transacciones electrónicas. [Tesis de maestría. Universidad de Cuenca].

Orús, A. (2023). ***Comercio electrónico en el mundo***. https://es.statista.com/temas/9072/comercio-electronico-en-el-mundo/#topicOverview

Parada, D., Florez, A., & Gómez, U. (2018). Análisis de los componentes de la seguridad desde una perspectiva sistémica de la dinámica de sistemas. ***Información tecnológica, 29***(1), 27-38. http://dx.doi.org/10.4067/S0718-07642018000100027

Pozo, C., Reascos, R., & Minaya, R. (2023). Comercio electrónico y riesgos de seguridad de la información durante la pandemia de COVID-19. ***Revista Científica Arbitrada Multidisciplinaria PENTACIENCIAS, 5***(6). https://doi.org/10.59169/pentaciencias.v5i6.896

Salas-Rubio, M., & Ábrego-Almazán, D. (2024). Influencia de la seguridad y la confianza como antecedentes de la aceptación y uso del comercio electrónico. ***Innovar, 34***(91), 9-18. http://doi.org/10.15446/innovar.v34n91.110010

Vargas, Z. (2009). La investigación aplicada: una forma de conocer las realidades con evidencia científica. ***Revista Educación, 33***(1), 155-165. http://www.redalyc.org/articulo.oa?id=44015082010

Vega, E. (2021). ***Seguridad de la Información***. Área de Innovación y Desarrollo,S.L.

Vega, V. (2013). Comercio electrónico y protección de datos. ***Revista de Estudios Económicos y Empresariales, 25***, 207-209. https://dehesa.unex.es/bitstream/10662/1368/1/0212-7237_25_205.pdf