UNIVERSIDAD POLITÉCNICA SALESIANA
SEDE GUAYAQUIL

CARRERA DE ADMINISTRACIÓN DE EMPRESAS

SEGURIDAD DIGITAL EN LA COMPRA DE PRODUCTOS POR PLATAFORMAS ONLINE: CONFIANZA Y PROTECCIÓN PARA LOS CONSUMIDORES GUAYAQUILEÑOS

Trabajo de titulación previó a la obtención del

Título de Licenciado/a en Administración de Empresas

AUTORES: RUIZ ESTUPIÑAN ROBERTO MAELO

TUTOR: CUEVA ESTRADA JORGE MANUEL

Guayaquil-Ecuador

2026

Resolución CS N°283-10-2025-09-17

CERTIFICADO DE RESPONSABILIDAD Y AUTORÍA DEL TRABAJO DE TITULACIÓN

Yo, Roberto Maelo Ruiz Estupiñan con documento de identificación N° 0943398925 manifiesto que:

Soy el autor y responsable del presente trabajo; y, autorizo a que sin fines de lucro la Universidad Politécnica Salesiana pueda usar, difundir, reproducir o publicar de manera total o parcial el presente trabajo de titulación.

Guayaquil, 19 de enero del año 2026

Atentamente,

Roberto Maelo Ruiz Estupiñan
C.I. 0943398925

UNIVERSIDAD POLITÉCNICA SALESIANA ECUADOR

SALESIANOS DON BOSCO

CERTIFICADO DE CESIÓN DE DERECHOS DE AUTOR DEL TRABAJO DE TITULACIÓN A LA UNIVERSIDAD POLITÉCNICA SALESIANA

Yo, Roberto Maelo Ruiz Estupiñan con documento de identificación No. 0943398925, expreso mi voluntad y por medio del presente documento cedo a la Universidad Politécnica Salesiana la titularidad sobre los derechos patrimoniales en virtud de que soy autor del Artículo Académico Seguridad digital en la compra de productos por plataformas online: confianza y protección para los consumidores Guayaquileños, el cual ha sido desarrollado para optar por el título de: Licenciado Administración de Empresa, en la Universidad Politécnica Salesiana, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente.

En concordancia con lo manifestado, suscribo este documento en el momento que hago la entrega del trabajo final en formato impreso y digital a la Biblioteca de la Universidad Politécnica Salesiana.

Guayaquil, 19 de enero del año 2026

Atentamente,

Roberto Maelo Ruiz Estupiñan
C.I. 0943398925

Calle Turuhuayco 3-69 y Calle Vieja • Casilla 2074 • Teléfono: (593) 74135250 • Correo electrónico: rector@ups.edu.ec • www.ups.edu.ec • Cuenca - Ecuador

CERTIFICADO DE DIRECCIÓN DEL TRABAJO DE TITULACIÓN

Yo, Jorge Manuel Cueva Estrada con documento de identificación N° 0918835224, docente de la Universidad Politécnica Salesiana, declaro que bajo mi tutoría fue desarrollado el trabajo de titulación: Seguridad digital en la compra de productos por plataformas online: confianza y protección para los consumidores Guayaquileños, realizado por Roberto Maelo Ruiz Estupiñan con documento de identificación N° 0943398925, obteniendo como resultado final el trabajo de titulación bajo la opción Artículo Académico, que cumple con todos los requisitos determinados por la Universidad Politécnica Salesiana.

Guayaquil, 19 de enero del año 2026

Atentamente,

Jorge Manuel Cueva Estrada
C.I. 0918835224

Resolución CS N°283-10-2025-09-17

AGRADECIMIENTO

Quiero expresar mi más sincera gratitud a Dios, por haberme brindado fortaleza, sabiduría y perseverancia a lo largo de este proceso, permitiéndome cumplir con cada etapa y alcanzar la culminación de esta tesis. Tambien le agradezco a mi madre por su apoyo incondicional, comprensión y motivación constante.

Finalmente, quiero expresar mi más grande y sincero agradecimiento a mi tutor licencido master Jorge Manuel Cueva Estrada por su orientación, colaboración y valioso apoyo académico, los cuales fueron fundamentales para el desarrollo y culminación de la presente tesis.

Att. Roberto Maelo Ruiz Estupiñan

DEDICATORIA

El presente trabajo de investigación lo dedico principalmente a Dios, por brindarme la fortaleza, sabiduría y responsabilidad constante durante este proceso de titulación, permitiéndome alcanzar uno de los logros más importantes de mi vida, obtener mi titulo de licenciado profesional en la carrera Administración de Empresa.

A mis padres, por su amor incondicional, apoyo constante y sacrificio, que han sido el pilar fundamental para alcanzar este logro. De igual manera, le dedico este logro a mis hermanos, por estar siempre presentes y brindarme su apoyo en todo momento a lo largo de esta etapa de mi vida.

Y a todas las personas externas que me brindaron su ayuda, apoyo y colaboración durante el desarrollo de este trabajo de investigación.

Att. Roberto Maelo Ruiz Estupiñan

Seguridad digital en la compra de productos por plataformas online: confianza y protección para los consumidores Guayaquileños

Digital security when buying products through online platforms: trust and protection for consumers in Guayaquil

Resumen:

El ámbito digital moderno, impulsado por el uso masivo de las plataformas digitales, ha favorecido el ascenso sostenido del comercio electrónico (CE) en el Ecuador. No obstante, este desarrollo también ha incrementado los riesgos asociados a fraudes, estafas digitales. En este contexto, el objetivo del presente trabajo fue analizar la seguridad digital en la compra de productos por plataformas online logrando confianza y protección en los clientes guayaquileños. Para ello, se desarrolló un estudio con enfoque cuantitativo-cualitativo. Se aplicaron encuestas a 384 consumidores que utilizan las plataformas digitales, con el fin de identificar las principales circunstancias de riesgo y vulnerabilidad que enfrentan los consumidores al realizar la adquisición de productos mediante compras digitales y determinar los niveles de confianza que los consumidores perciben de las plataformas digitales. Adicionalmente, se realizaron entrevistas a expertos en ciberseguridad para evaluar los sistemas de seguridad que las plataformas implementan para la protección de datos y transacciones de pago. Los principales resultados evidencian que más del 51% de los encuestados mantiene una percepción neutral de confianza al realizar compras en línea. además, los principales riesgos identificados corresponden a fraudes y estafas digitales. En conclusión, la seguridad digital influye de manera importante en la confianza de los consumidores, siendo necesaria la adaptación de estándares de ciberseguridad, orientados a fortalecer un entorno más seguro para el comercio electrónico en el Ecuador.

Abstract:

The current digital environment, driven by the widespread use of digital platforms, has fostered the sustained growth of e-commerce in Ecuador. However, this development has also increased the risks associated with fraud and online scams. In this context, the objective of this study was to analyze digital security in online purchases, aiming to build trust and protection among consumers in Guayaquil. To this end, a mixed-methods (quantitative and qualitative) study was conducted. Surveys were administered to 384 consumers who use digital platforms to identify the main risks and vulnerabilities they face when purchasing products online and to determine the levels of trust consumers place in these platforms. Additionally, cybersecurity experts were interviewed to evaluate the security systems that platforms implement for data protection and payment transactions. The main findings show that over 51% of respondents maintain a neutral perception of trust when making online purchases. Furthermore, the main risks identified are digital fraud and scams. In conclusion, digital security significantly influences consumer confidence, making it necessary to adapt cybersecurity standards aimed at strengthening a safer environment for e-commerce in Ecuador.

Palabras Claves: Seguridad digital, Plataformas digitales, Comercio Electrónico, ciberseguridad, protección informática.

Keywords: Digital security, Digital platforms, Electronic Commerce, Cybersecurity, Computer protection.

1. Introducción

De acuerdo con Fernández Muerza (2022) la evolución del internet y las tecnologías digitales, han sido un factor clave para el diseño de las plataformas virtuales orientadas a la automatización de tareas rutinarias, buscando la reducción del tiempo. Estas herramientas se han vuelto un recurso necesario para el desarrollo de actividades tanto en el ambiente personal como profesional.

Según señala Quintero-López (2020) la presencia de plataformas comerciales electrónicas se posiciona como una solución para la adquisición de productos y ofrecimiento de servicios, mediante páginas virtuales y aplicaciones móviles. Estas plataformas además de brindar diferentes ofertas de productos y servicios, también permite a sus usuarios conocer los aspectos del producto de su interés, lo que otorga poder al cliente, permitiéndoles tomar decisiones más informadas. De ahí el crecimiento del comercio digital a escala mundial.

En este sentido, es importante que los usuarios sepan identificar que las plataformas en las cuales van a solicitar la adquisición de mercadería o servicio, esté antes, certificada por todos los ámbitos legales y comerciales, que validen su autenticidad, lo que da credibilidad al sitio y brinda confianza a los usuarios (Véliz Intriago, 2024). Sin embargo, los consumidores están expuestos a posibles escenarios de fraudes cibernéticos, estafas comerciales y publicidad engañosa. Si bien, la tecnología ha sido un medio que ha revolucionado y optimizado el ámbito comercial, continúa siendo un instrumento que debe manejarse de manera responsable (Chiliquinga-Villacis y Redrobán-Barreto, 2025). De lo contrario, su uso inadecuado puede exponer a los consumidores a riesgos como fraudes, engaños y pérdidas de recursos financieros y personales (Santamaría-Mendoza et al, 2024).

Las plataformas digitales comerciales, fueron diseñadas con la finalidad de proporcionar un acceso directo a la información de productos y servicios. Sugiriendo un aporte significativo para el desarrollo económico y comercial tanto nacional como internacional. (Heredia y Villarreal, 2022). La emergencia sanitaria mundial provocada por el covid-19, ocurrida aproximadamente hace cinco años, generó efectos significativos tanto en la sociedad como en el ámbito empresarial. Si bien las plataformas digitales ya existían antes de la pandemia, este

contexto aceleró de manera considerable su evolución y adopción. Durante ese periodo, las restricciones de movilidad limitaron la interacción presencial para la adquisición de productos y el acceso a servicios, lo que ocasionó una disminución sostenida de las ventas y, en consecuencia, una reducción de los ingresos empresariales. Esta situación resulta relevante de analizar, considerando que muchas organizaciones no contaban con planes de contingencia ni estrategias que les permitan subsistir frente a ese problema emergente (Becerra Molina et al, 2021), sin embargo, ese mismo contexto se convirtió en un entorno fértil para el desarrollo del comercio electrónico y de las aplicaciones móviles.

En Ecuador, en los últimos años, las plataformas comerciales han presentado un incremento significativo en su demanda por parte de los consumidores. Estas plataformas les permiten a los negocios ampliar su proyección comercial a nuevos mercados y público, optimizando eficazmente el tiempo de venta y mejorando la comunicación con sus clientes, lo cual genera un crecimiento sostenible a lo largo del tiempo (Mera Servigón, 2021). El uso de plataformas digitales ha facilitado la automatización de ventas y la elaboración de nuevas ofertas. Como resultado, los negocios han logrado fortalecer su posicionamiento, adaptarse a las nuevas tendencias del mercado (Molina Tenesaca et al, 2025).

Según señala Tunqui Cruz (2024). A pesar de todas las bondades que sugiere el uso de herramientas y plataformas digitales, la seguridad en estos entornos es un elemento que aún no está atendido adecuadamente, por parte de negocios, emprendimientos e incluso empresas, por lo que a continuación se propone las siguientes preguntas de investigación: ¿Cómo influye la seguridad digital en la compra de productos por plataformas online en Guayaquil?; ¿Qué sistemas de seguridad electrónica están usando en la actualidad en Ecuador?; ¿En qué medida los sistemas de ciberseguridad de las plataformas digitales reducen los fraudes y estafas digitales en el país?; ¿Cuál es el efecto de las normas y regulaciones legales sobre la seguridad del consumidor en plataformas digitales en Ecuador?

1.1. Sistemas de seguridad Electrónica

La seguridad electrónica se compone de un conjunto de implementos, acciones y mecanismos destinados para el resguardo de los datos informáticos de los sistemas operativos.

Frente a posibles riesgos o ataques cibernéticos. Su principal objetivo es resguardar la seguridad de los dispositivos, permitiendo a los usuarios y a la empresa operar de manera eficaz. Estos sistemas de protegen las siguientes herramientas: Servidores, sistemas de monitoreo, controles de acceso informáticos y unidades de videovigilancia digital (Aznar-Martínez et al, 2024).

Los sistemas de seguridad electrónicas ofrecen múltiples beneficios a la protección informática y garantiza gestiones estables de las organizaciones en entornos digitales. Estos sistemas reducen proporcionalmente el riesgo de fugas, alteraciones o accesos no autorizados. A continuación, se presentan sistemas (malware, ransomware y virus informáticos) softwares que afectan los sistemas electrónicos y son utilizados parcialmente para el hurto o robo de datos informáticos. Los sistemas de seguridad funcionan en la verificación de posibles ataques cibernéticos y permitiendo una solución inmediata. (Salazar Larico, 2021).

Diversas fuentes destacan la necesidad de la seguridad informática, la cual se considera una prioridad. Las plataformas digitales, debido a su crecimiento y alta demanda, deben proporcionar sistemas de ciberseguridad que aseguren la protección e integridad de los datos almacenados, mejorando su rendimiento operativo (Tayupanta et al, 2024). En este contexto, es necesario que los sistemas de seguridad digital implementen protocolos de certificación y verificación, ofreciendo alternativas seguras para el uso de las plataformas. Asimismo, se requiere la incorporación y uso de comandos, sistemas y módulos especializados en la protección de datos y servidores y que estos refuercen su seguridad. Por tal razón, la (SE) debe mantenerse en constante monitoreo, con la finalidad de respaldar la seguridad de las plataformas automatizadas: financieras, comerciales y laborales. (Juca-Maldonado y Medina-Peña, 2023).

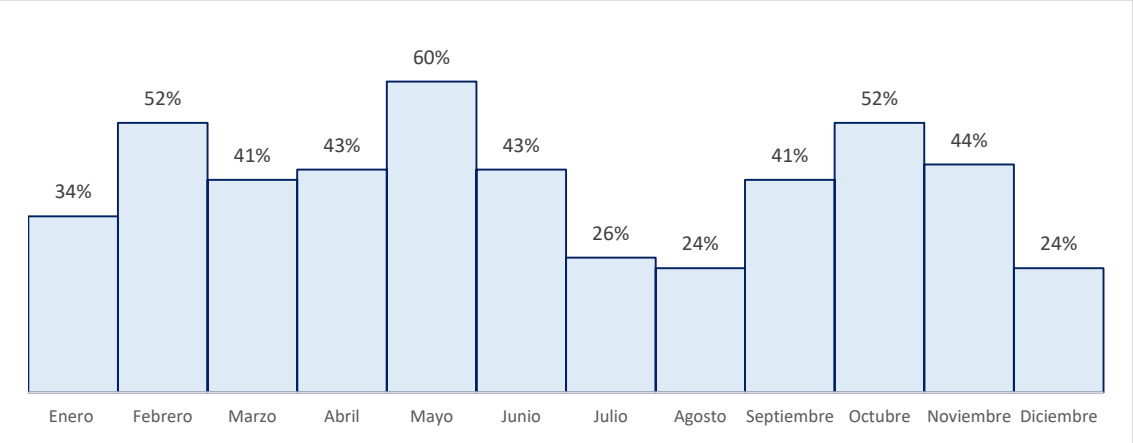
1.1.1. Efectos positivos de la seguridad electrónica

Los sistemas de seguridad electrónica y mecanismos de monitoreo en las plataformas digitales. Sirve para brindar mayor protección a la información de los usuarios, garantizando el correcto uso de los procesos de las transacciones (financieras-comerciales). Asimismo, estos instrumentos se encargan de la identificación de posibles amenazas cibernéticas y ofrecen alternativas de posible mejoría. Estos sistemas también deben cumplir con las normas legales electrónicas (Peñarrieta, 2024).

López-Anchala y Ordóñez-Parra (2024), presentan un estudio sobre la ciberseguridad que se ha vuelto un factor importante para la protección de los sistemas electrónicos ante posibles amenazas cibernéticas. Se presenta un gráfico sobre el rendimiento protección de la ciberseguridad en las plataformas digitales. Los datos analizados pertenecen al año 2024 y se presentan mediante una proyección mensual porcentual, lo que permite evaluar la evolución progresiva del nivel de protección de los sistemas digitales. Como se observa en la Figura 1, una tendencia en el rendimiento de la ciberseguridad durante el año 2024, la cual evidencia los niveles de protección de los sistemas digitales.

Figura 1:

Porcentaje de Efectividad en la seguridad digital en las plataformas comerciales (2024).

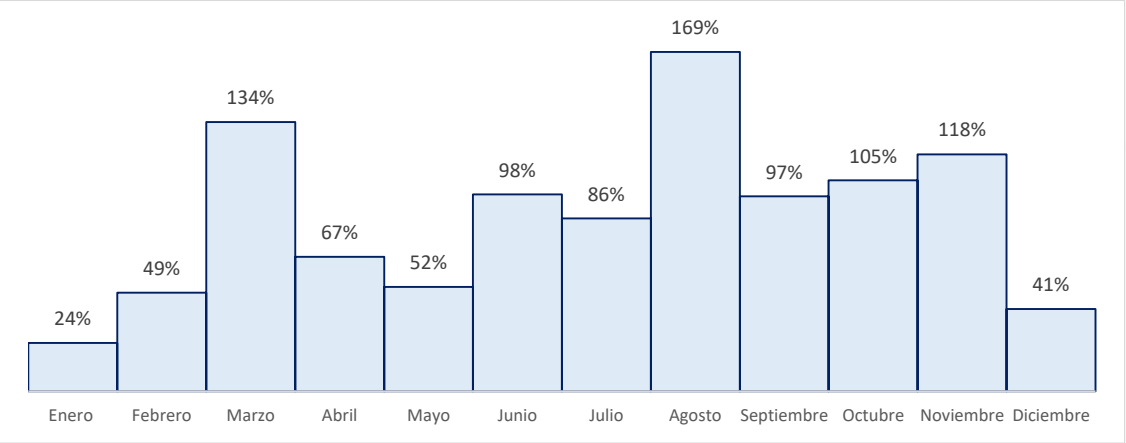


Nota, La figura representa la evolución mensual del nivel de protección de los controles de ciberseguridad implementados en plataformas digitales comerciales. Fuente: López-Anchala y Ordóñez-Parra (2024).

Según lo explicado por Calle-Tenesaca (2024), la ciberseguridad es un factor necesario en para el resguardo de los datos financieros en las organizaciones comerciales. Destaca que los sistemas digitales seguros permiten la prevención de posibles amenazas informáticas, reduciendo su riesgo para las plataformas. Asimismo, se presenta una proyección mensual expresada en porcentajes correspondiente al año 2024, la cual evidencia los niveles de protección de los sistemas digitales. Tal como se observa en la Figura 2, confirma que las estrategias de seguridad adoptadas altas y bajas del nivel de protección y disminuyen proporcionalmente los riesgos electrónicos, especialmente en entornos de comercio digital.

Figura 2:

Porcentaje de evolución del nivel de protección de los datos financieros en las plataformas comerciales (2024)

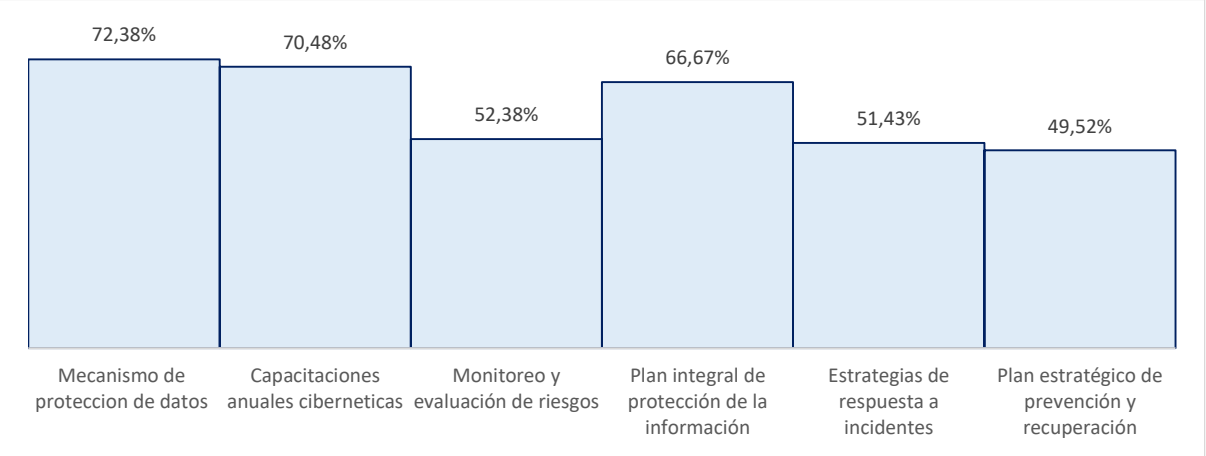


Nota, La figura muestra la evolución mensual del nivel de seguridad de los datos financieros mediante la aplicación de sistemas de ciberseguridad en sus plataformas. Fuente: Calle-Tenesaca (2024).

Según el informe de Bravo (2025), las organizaciones en Ecuador implementan diversas medidas de ciberseguridad orientadas a la reducción de incidentes de amenazas digitales (se realizó una evaluación a 150 empresas nacionales). Los porcentajes presentados reflejan la proporción de las empresas que reportan la aplicación de cada medida. Entre las principales medidas para la reducción de incidentes de amenazas cibernéticas se identifican las siguientes: la figura 3 y 4 presenta mediante una proyección porcentual de las medidas de ciberseguridad aplicadas en Ecuador y su objetivo de protección de los sistemas digitales.

Figura 3:

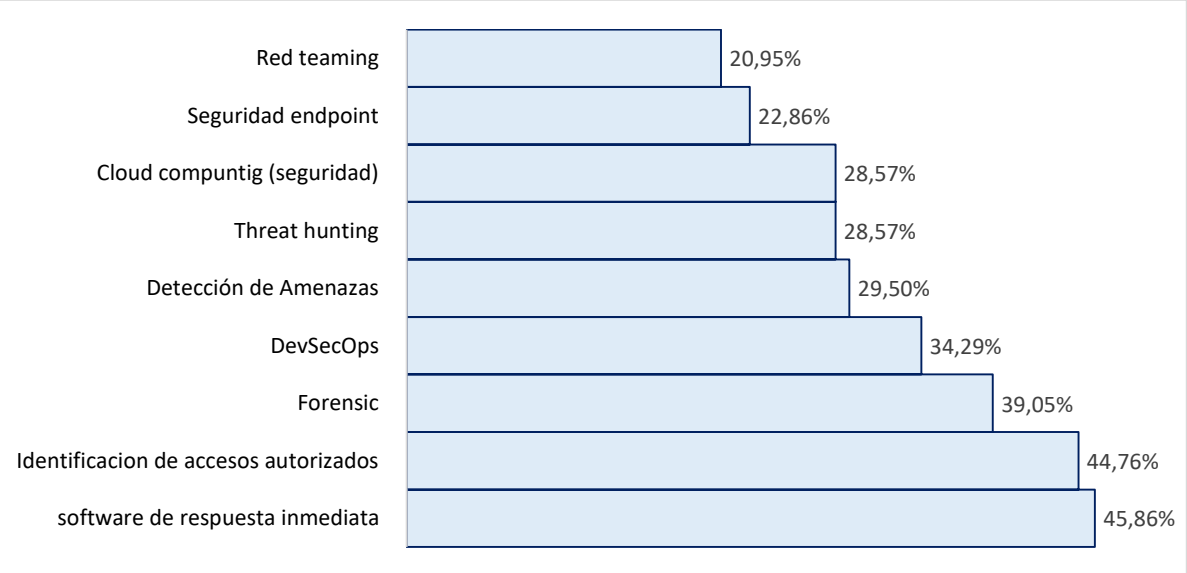
Nivel de implementación de medidas de ciberseguridad en plataformas digitales en Ecuador (2025)



Nota, Los porcentajes representan la proporción de organizaciones ecuatorianas que han implementado cada medida de ciberseguridad con el objetivo de reducir incidentes digitales. Fuente: Bravo (2025).

Figura 4:

Nivel de protección de las medidas de ciberseguridad en plataformas digitales en Ecuador (2025)



Nota, La figura 4 representa la distribución porcentual del nivel de protección de la ciberseguridad en plataformas digitales en Ecuador en el año 2025. Los hallazgos evidencian que gran parte de las organizaciones presentan un nivel alto de protección, lo que contribuye a la reducción de fraudes y estafas digitales. Fuente: Bravo (2025).

Los porcentajes presentados en las figuras de cada estadística no representan una distribución total, sino valores independientes asociados a periodos temporales o a la implementación de medidas específicas.

1.1.2. **Seguridad Electrónica en Ecuador**

La seguridad electrónica en el país, se presenta mecanismos para la protección informática en espacios digitales. Sin embargo, este recurso propone varios sistemas y mecanismos de seguridad para las plataformas digitales (Veloz Segura, 2025). A continuación, se presentas los siguientes sistemas:

Sistema de alarma electrónica, herramienta encargada de localizar, detectar posibles alertas de riesgos en los servidores en espacios tecnológicos públicos o privados. Resguardan la informática en los sistemas electrónicos. Esta herramienta funciona a través de monitoreos digitales, se presenta en la plataforma cuando registran alguna anomalía sospechosa. Enviando señales de alerta a los servidores principales y que estos ejecuten medidas de solución. (López Loja, 2023).

Sistema de acceso electrónico verificados, aquel que regula la supervisión de las plataformas por parte de los usuarios, garantizando que los accesos sean permitidos por la autorización de los propietarios, esto ayuda a la seguridad de la información y que recursos no sea extraídos por agentes no autorizados. Este tipo de herramientas utiliza métodos como códigos, cifrados, contraseñas y lectores biométricos (reconocimiento de voz, huella o facial) estos comandos son aplicados tanto en plataformas, aplicaciones y portales web (Estrella Murillo, 2024).

Sistemas de seguridad económica o financiera, herramienta diseñada para la protección de los servidores en entidades financieras (Bancos, instituciones monetarias y cooperativas económicas y crediticias) esta herramienta ayuda al resguardo informático de cuentas bancarias, tarjetas (crédito o débito) y pólizas financieras. Busca la reducción de posibles intentos de robos o fraudes en la actualidad. (Astudillo-Romero y Torres-Negrete, 2024).

Sistemas de ciberseguridad automatizados, conjunto de herramientas digitales, procedimientos destinados a la defensa de los ecosistemas virtuales, frente a posibles riesgos cibernéticos. Brinda solución a posibles riesgos en los sistemas, la ciberseguridad implementa medidas como: antivirus, firewalls, autenticación electrónica, monitoreos de detección. Estos sistemas han presentado un impacto significativo para las plataformas digitales en la actualidad (Santillán Molina, 2024).

1.1.3. Regulaciones y seguridad del consumidor

Según Minaya Macias et al (2023), explica de forma profesional sobre las normas y estándares en la gestión de los sistemas electrónicos en la protección informática de los consumidores, verificando su rendimiento en el Ecuador. Las normas legales en los ambientes electrónicos son reglamentos que se deben implementar en los procesos autónomos de las plataformas, ofreciendo mayor seguridad en los entornos laborales. Normas como las siguientes (Ordóñez Córdova, 2024):

- ✓ Norma legal Orgánica de Seguridad y Vigilancia (Pública-Privada).
- ✓ Norma legal de mercantilización electrónicas y Firmas electrónicas.
- ✓ Norma legal Orgánica para la transformación Digital y Audiovisual.
- ✓ Normas legal Orgánica de Seguridad Digital.

La implementación de las normas y regulaciones en la protección informática, según la norma ISO 27001 (estándar de seguridad informática) permite establecer medidas para mejorar el rendimiento de los sistemas, esta aumenta mejora la seguridad en los medios digitales en espacios laborales.

Según el criterio de Lucero (2023). En efecto la ciberseguridad en los sistemas electrónicos, regularizadas por entidades gubernamentales, son encargados del resguardo y protección de los datos (personales y financieros). La seguridad electrónica brinda un resguardo seguro para las plataformas digitales. Por otro lado, los reglamentos de ciberseguridad exigen a las aplicaciones plantear mecanismos encargados en el correcto almacenamiento de datos internos. Adicionalmente, estas regulaciones refuerzan el nivel de confianza que los consumidores perciben por las plataformas digitales (Silva Andrade et al, 2024).

La ley orgánica de protección de datos, establecen decretos para mejorar el rendimiento en las prácticas de protección informática, para las nuevas tecnologías como: blockchain, zero trust security, firewall, chatbots inteligentes, RPA (automatización robótica de procesos). Son programas que requieren una constante revisión sistemática y nuevas de protección en sus servidores y establecer monitoreos en cumplimiento de las normativas legales en protección informática en los entornos tecnológicos, fortaleciendo accesos seguros para los usuarios (Moreira Moreira, 2024). Es esencial implementar controles, realizar auditorías periódicas y establecer marcos normativos que aseguren la seguridad e integridad en sistemas digitales, minimizando los riesgos de amenazas electrónicas (Cedeño Villacís, 2022).

La presente investigación, se platea como objetivo analizar la seguridad digital en la compra de productos por plataformas online, logrando mejora la percepción de confianza y protección en los clientes guayaquileños. El presente estudio es importante porque aporta conocimiento sobre la ciberseguridad en las plataformas digitales, verificando su utilidad en los mecanismos electrónicos de protección de datos informáticos en los entornos virtuales, convirtiéndolos en medios seguros (Bueno Valero, 2022).

2. Metodología

El estudio se desarrolló bajo un enfoque mixto cualitativo-cuantitativo (Medina Romero, 2023) también se integraron los métodos inductivo-deductivo, con el fin de reunir evidencia necesaria para lograr el objetivo general que guio el estudio: analizar la seguridad digital en la compra de productos por plataformas online, logrando mejorar la percepción de confianza y protección en los clientes guayaquileños.

Para lograr el cumplimento del primer y segundo objetivo específico: Identificar las principales circunstancias de riesgo y vulnerabilidad que enfrentan los consumidores al realizar la adquisición de productos mediante compras digitales y determinar los niveles de confianza que los consumidores brindan a las plataformas digitales. Para la parte cuantitativa, se elaboró un cuestionario de 11 preguntas de opción de respuestas cerradas basadas en la escala de Likert (Astudillo Torres, 2021). El cuestionario de preguntas fue desarrollado mediante la plataforma de Microsoft Forms desde mi cuenta institucional, siendo que los resultados que se obtengan

serán utilizados para fines académicos y dichos datos reposarán en mi cuenta institucional de la Universidad Politécnica Salesiana. Las encuestas se realizaron mediante modalidad virtual, durante un periodo de 15 días a partir del 11/12/2025 hasta el 18/12/2025.

Según el Instituto Nacional de Estadística y Censos (INEC) (2025), la población ecuatoriana de usuarios activos que utilizan servicios en internet es de 12 400 000 millones de personas, de las cuales, el estudio afirma que el 3% de los ciudadanos corresponde a personas que han comprado de forma digital, dando como resultado una población de 372 000 ecuatorianos que han realizado transacciones de e-commerce en Ecuador. Para una confianza del 95% en los resultados y tolerar un error máximo del 5%, el tamaño de muestra mínima debe ser de 384 usuarios (Reyes et al., 2013).

Mientras que, para la parte cualitativa, se empleó el desarrollo de un cuestionario de preguntas abiertas, dirigido para entrevistar a profesionales en seguridad digital y sistemas operativos computacionales en el Ecuador. Se diseñó el cuestionario de entrevista con la finalidad del cumplimiento del segundo objetivo específico del artículo: Evaluar los sistemas de seguridad que las plataformas implementan para la protección de datos y transacciones de pago.

Las entrevistas se realizaron de forma virtual, mediante un correo electrónico institucional, a partir del 15/12/2025 hasta el 18/12/2025. Para el desarrollo del estudio se contó con la participación de tres expertos, cuya experticia fue valorada en función de su formación académica de cuarto nivel y su especialización en áreas relacionadas con sistemas computacionales y la ciberseguridad. Los expertos poseen títulos de ingeniería y posgrado, los cuales respaldan su conocimiento teorico y técnico, lo cual garantiza criterios académicos y profesionales pertinentes para la validación y el análisis de la investigación.

3. Resultados

3.1 Encuestas

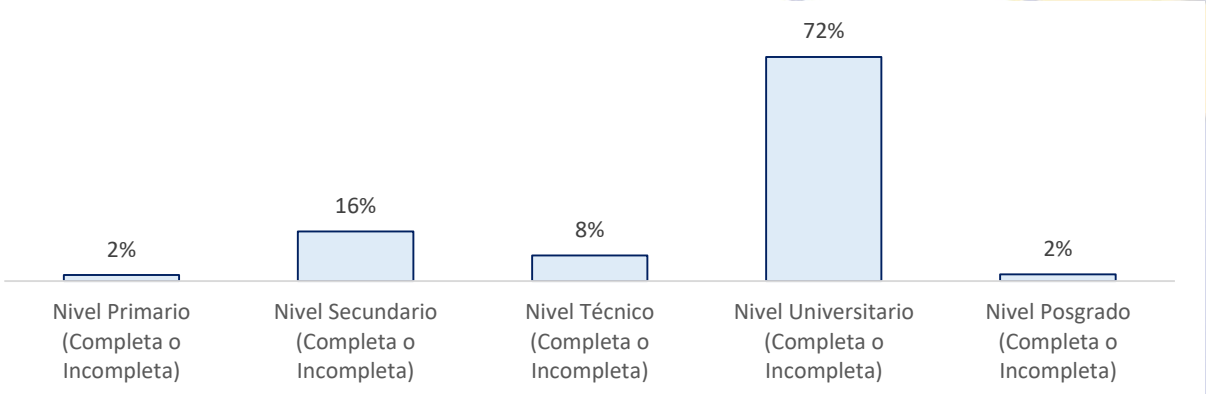
A continuación, se presentan los resultados de las respuestas por parte de la población que participó en la encuesta. Lo cual, de los 384 participantes pronosticados, se alcanzó un total de 403 respuestas. Se muestran los resultados:

Una vez realizado el proceso de levantamiento de información determinado por las herramientas de investigación (entrevista y encuesta). Detallo los resultados obtenidos por parte de las encuestas a los consumidores que usan el comercio electrónico, lo que evidencia resultados significativos en cuanto a la percepción de nivel de confianza que los consumidores perciben en las plataformas comerciales, así como la identificación de los riesgos que presentan en este tipo de servicio y evaluar los sistemas de seguridad que las plataformas implementan para la protección de datos y transacciones de pago.

En relación con los resultados sociodemográficas, la muestra estuvo conformada por 222 hombres, 178 mujeres y 3 participantes que prefirieron no decir su sexo. En cuanto a las edades: el 82% de los encuestados se ubicó en el rango de 18-27 años; el 13% correspondió al rango de 28-43 años, el 4% correspondió al rango de 44-59 años y apenas el 1% indicó tener 60 años o más. Estos resultados permiten presentar las características sociodemográficas de la población encuestada, las cuales, con sus respuestas, se pueden identificar los hallazgos vinculados al cumplimiento de los objetivos de la investigación.

Figura 5:

Nivel de educación de los encuestados



Nota, La figura 5 identifica el nivel de educación de los encuestados poseen (completa-incompleta). Con se puede observar el 72% de los encuestado presenta un nivel de educación universitario.

Preguntas relacionadas al cumplimiento del objetivo Especifico 1: Identificar las principales circunstancias de riesgo y vulnerabilidad que enfrentan los consumidores al realizar la adquisición de productos mediante compras digitales.

Tabla 1:

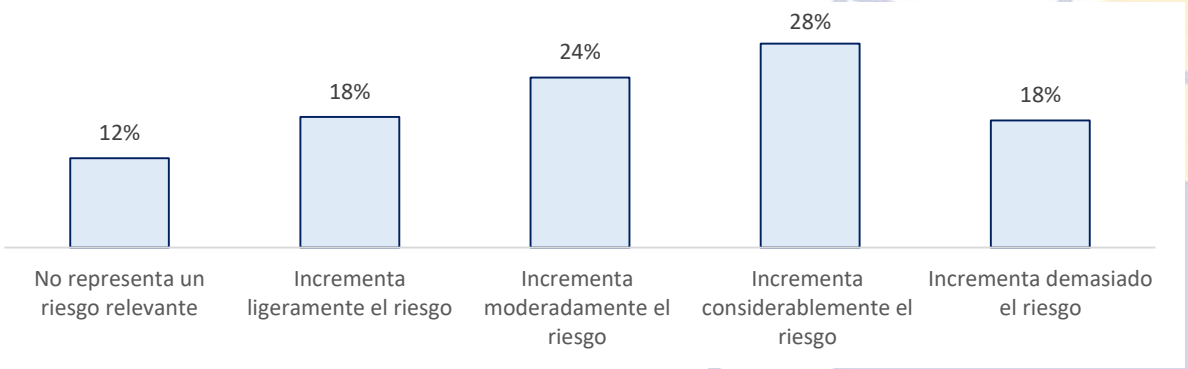
Principales riesgos percibidos al realizar una compra de un producto o servicio a través de las plataformas digitales

Opciones de Respuestas	Resultados
Dificultad para realizar devoluciones o reclamos	5%
Incumplimiento en el tiempo de entrega del producto	7%
Fraudes o estafas digitales durante el proceso de pago	23%
Robo o uso indebido de datos personales y financieros	24%
Recibir un producto defectuoso o diferente a lo promocionado	**41%**

Nota, La Tabla 1 como se puede observar, el 41% de los encuestados percibió que recibir un producto defectuoso o no diferente es un riesgo que afecta las compras a través de las plataformas digitales.

Figura 6:

Percepción sobre la falta de claridad en la información del producto como factor de riesgo en las compras digitales por parte de los consumidores



Nota, El 28% de la población considera que incrementa considerablemente su riesgo.

Tabla 2:

Principales riesgos que generan vulnerabilidad para los consumidores al comprar en línea

Opciones de Respuestas	Resultados
Bajo control de calidad de los productos	3%
Poco experiencial de estas herramientas	15%
La falta de garantías sobre los envió o entrega	22%
Desconocimiento del funcionamiento de la plataforma	22%
El riesgo de fraude y estafas virtuales	**38%**

Nota, Se observa que el 38% de los encuestados eligieron que el riesgo de fraude y estafas virtuales es aquellos por lo que se sienten vulnerables al comprar en línea.

Tabla 3:

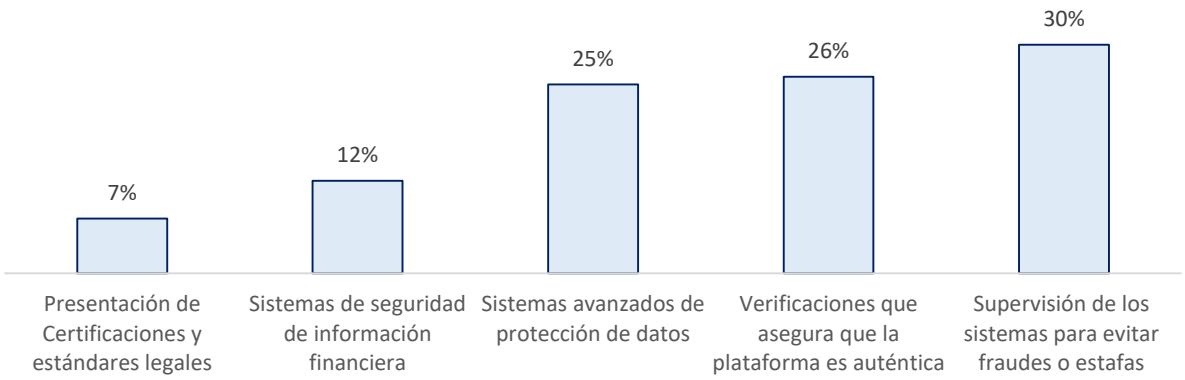
Factores que incrementa el riesgo de fraude o engaño en las compras y adquisición de servicio online

Opciones de Respuestas	Resultados
Escasa presencia de educación digital	10%
La falta de sistemas adecuados de ciberseguridad	10%
La ausencia de calificaciones, reseñas o referencias	12%
Falta de opiniones por otros usuarios verificados	17%
Uso de plataformas pocas conocidas en el internet	24%
Falta de verificación de los vendedores	**27%**

Nota, La tabla 3 como se puede observar, el 27% de los encuestados seleccionaron que la falta de verificación de los vendedores representa un incremento en el riesgo de fraude o engaños en las compras en las plataformas digitales.

Figura 7:

Mecanismos de seguridad relevantes para la reducción del riesgo percibido al adquirir productos a través de plataformas digitales en la ciudad de Guayaquil



Nota, La figura 7 como se puede observar, el 30% de los encuestados considera que el mecanismo de supervisión de los sistemas para evitar fraudes o estafas digitales desempeña un papel relevante en la reducción de riesgo en adquirir productos a través de las plataformas comerciales en la ciudad de Guayaquil.

Preguntas relacionadas al cumplimiento del objetivo específico 2: Determinar los niveles de confianza que los consumidores perciben a las plataformas digitales.

Tabla 4

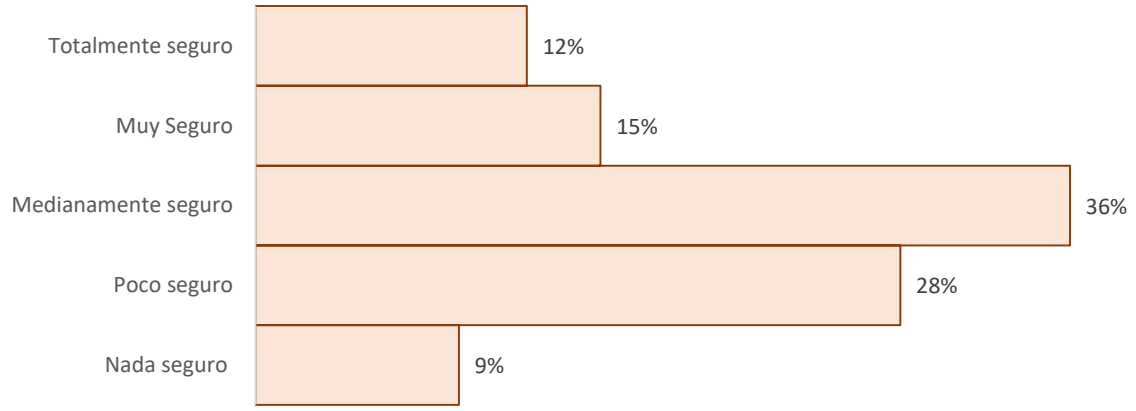
Nivel de confianza del consumidor en la compra de productos y servicios mediante plataformas digitales

Opciones de Respuestas	Resultados
Totalmente confiado	11%
Muy confiado	15%
Neutral	**51%**
Poco confiado	20%
Nada confiado	3%

Nota, La tabla 4 como se puede observar, el 51% de los encuestados adoptaron una postura neutral. Evidenciando que gran parte de los encuestados están en una posición neutral de confianza en comprar productos mediante las plataformas digitales.

Figura 8:

Percepción de seguridad al ingresar datos financieros "cuenta bancaria, tarjeta de crédito y billeteras electrónicas (De una, PayPal)" en las plataformas de pago digitales



Nota, La figura 8 como se puede observar, el 36% de los encuestados respondieron que se siente medianamente seguros al ingresar sus datos financieros en las plataformas digitales. Lo que nos evidencia que gran parte de la población tiene percepción de seguridad parcial en compartir su información financiera en las plataformas digitales.

Tabla 5

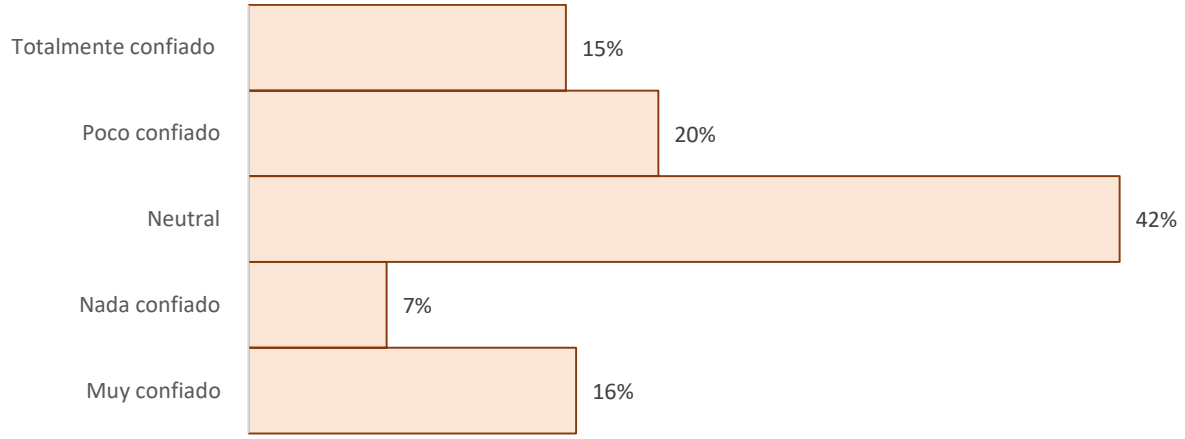
Importancia de la reputación de las plataformas digitales como un factor determinante para la confianza y seguridad al realizar compra en línea por parte de los consumidores

Opciones de Respuestas	Resultados
Totalmente de acuerdo	**37%**
De acuerdo	28%
Neutral	27%
En desacuerdo	5%
Totalmente en desacuerdo	3%

Nota, La tabla 5 como se puede observar, el 37% contestaron que totalmente de acuerdo. Evidenciando que gran parte de los encuestados consideran que la buena reputación de las plataformas digitales es un factor muy importante que les genera una percepción de confianza efectiva en su seguridad a la hora de comprar un producto y adquirir un servicio online.

Figura 9:

Nivel de confianza en la protección y uso de los datos personales (nombre, identificación, dirección y teléfono) por parte de las plataformas digitales



Nota, La figura 9 como se puede observar, el 42% de los encuestados se siente en un nivel neutro de confianza que perciben por parte de las plataformas digitales, en que estas no utilizarán o compartirán sus datos personales sin su consentimiento. Lo que indica que gran parte de los encuestados no se siente confiados al compartir sus datos personales en medios públicos como las plataformas digitales.

Tabla 6:

Mecanismos efectivos para mejorar la seguridad digital y generar un aumento de confianza en las plataformas digitales en la ciudad de Guayaquil

Opciones de Respuestas	Resultados
La supervisión constante de las plataformas digitales	9%
Las empresas deben mostrar certificaciones que garanticen la seguridad del sitio o la aplicación web	11%
Monitoreos gubernamentales más rígidos	11%
Sistemas de pagos más protegidos y efectivos	22%
Mayor verificación de la identidad del vendedor	22%
Mayor protección de seguridad contra posibles fraudes	**25%**

Nota, Para finalizar la tabla 6, como se puede observar el 25% de los encuestados consideran que la medida de "mayor protección de seguridad contra posibles fraudes" es la alternativa más efectiva para mejorar la seguridad digital en las plataformas digitales, ofreciendo un ascenso en

la identificación de seguridad por parte de los consumidores guayaquileños que utilizan este tipo de servicio online.

3.2 Entrevista

A continuación, se presenta las opiniones de la entrevista de los 3 expertos de la Universidad Politécnica Salesiana:

En fusión al cumplimiento del objetivo Especifico 3: Evaluar los sistemas de seguridad que las plataformas implementan para la protección de datos y transacciones de pago.

En resumen, en la pregunta 1: ¿Cuáles son los principales mecanismos de seguridad digital que, desde su experiencia, deben implementar las plataformas digitales para garantizar la protección de los datos personales y financieros de los consumidores en Guayaquil? Los entrevistados concuerdan en que la ciberseguridad se encarga de la protección de datos informáticos, tanto personales como financieros. Los expertos coinciden en la necesidad de aplicar mecanismos y estándares que se encarguen de la protección de los sistemas operativos; entre los mencionados tenemos: Los cifrados de datos en tránsito y en reposo (TLS 1.2/1.3 y AES-256), la importancia de la aplicación de monitoreos continuos (SIEM), uso de firewalls y WAF para la detección de amenazas, así como la adopción de protocolos de seguridad informática como (ISO/IEC 27001 y OWASP).

Por otro lado, en la pregunta 2: ¿Qué protocolos o estándares de ciberseguridad considera indispensables para evaluar y proteger las transacciones de pago financieros realizados a través de las plataformas digitales? Los entrevistados proponen que los estándares que permiten una mejor protección en las transacciones de pagos son: Principalmente, los PCI DSS que constituyen en la protección de los sistemas electrónico y el almacenamiento de los registros financieros; también se deben utilizar sistemas de cifrado automatizados como los TLS/SSL, que son necesarios porque garantizan el resguardo de los medios tecnológicos, la ISO/IEC 27001, estándares que permiten evaluar la seguridad de un sistema electrónico. Por ultimo menciona la importancia de que los medios digitales implementen marcos de seguridad como

el NIST Cybersecurity Framework, que contribuye en evaluar los niveles de seguridad de las plataformas digitales.

Siguiendo, con la pregunta 3: ¿Qué recomendaciones técnicas propondría para fortalecer los sistemas de seguridad de las plataformas digitales? Los entrevistados recomendaron que, para mejorar los sistemas de seguridad en las plataformas digitales, se deben tener en cuenta el uso de cifrado fuerte de datos en tránsito (TLS 1.2/1.3) y en reposo (AES-256) y exigir autenticación multifactor en todos los accesos electrónicos. Asimismo, se enfatice en la aplicación de controles de acceso, eliminar configuración o cuentas irregulares. Los expertos detallan la importancia que las plataformas cumplan con los mecanismos de seguridad en las formas de pagos digitales, asi como aplicar medidas como el DevSecOps y SAST/DAST. Finalmente, el establecimiento de módulos de respuesta rápida ante posibles incidentes, alineados con estándares como NIST SP 800-61, permite una reacción eficaz ante posibles eventos inesperados, fortaleciendo la seguridad en las plataformas digitales.

Continuando, en la pregunta 4: Desde su punto de vista profesional, ¿cómo evalúa la efectividad de los mecanismos de seguridad digital que utilizan las plataformas digitales en la actualidad? Los entrevistados explican que los mecanismos de la seguridad digital han ido teniendo un rendimiento mejorado en su protección en los sistemas operativos. Gracias a la utilización de herramientas como: MFA (autenticación multifactorial), cifrados automatizados de seguridad, la WAF (Web Application Firewall), Application Firewall y los sistemas de gestión de seguridad informática en red.

Para finalizar, la pregunta 5: Desde su experiencia, ¿en qué medida los sistemas de ciberseguridad ayudan a las plataformas de comercialización en línea a evaluar su rendimiento de la protección de sus sistemas operativos, contribuyen a la reducción de fraudes y estafas en el país? Los entrevistados coinciden en que los sistemas de ciberseguridad determinan un factor clave en la protección de los sistemas electrónicos y en la posibilidad de reducción de ataques electrónicos. Estos sistemas permiten medir la efectividad de los controles de ciberseguridad que son aplicados en la protección informática y transacciones económicas no solicitadas. Asimismo, mecanismo de monitoreo en tiempo real, detecciones de anomalías, sistemas

antifraudes basados en análisis de comportamiento en los sistemas operativos. Estos mecanismos no solo reducen proporcionalmente las anomalías de fraudes, sino que promueven un ecosistema digital más seguro y protegido, siendo un beneficio para el e-commerce en el Ecuador.

3. Discusión

Según los resultados del presente estudio, más del 30% de los encuestados consideran que la supervisión constante de los sistemas electrónica encargados de la prevención de posibles fraudes y estafas es una de las medidas más efectivas para la protección de las plataformas digitales. En línea con ello, Portilla Paguay et al. (2025), concluyen con la importancia que los medios electrónicos, deben implementar mecanismos de protección y resguardo de sus sistemas operativos, con el fin de ofrecer soluciones oportunas frente a posibles ciberataques digitales.

En lo relacionado con el ingreso de datos financieros, los resultados evidenciaron que un 36% de los encuestados, respondieron que se siente medianamente seguros al ingresar sus datos financieros en las plataformas digitales, lo que evidencia que gran parte de la población mantiene una percepción de seguridad parcial en compartir estos datos. En este sentido, pero desde otro punto de vista, los resultados del estudio concuerdan con los informes de Endara Chamorro et al (2025), quienes en un estudio, sobre la importancia de los datos financieros en el Ecuador, basados en la aplicación de una encuesta a la población ecuatoriana, señalan que un 30% de los ecuatorianos considera necesario que los sistemas de seguridad en las plataformas digitales, protejan y resguarden adecuadamente sus datos financieros para qué no sean compartidos sus datos sin su consentimiento.

Según los resultados del presente estudio, se comprobó que más del 51% de los encuestados se ubica en una postura neutral de confianza al comprar productos o adquirir servicios mediante las plataformas digitales. En contraste, el informe elaborado por Infante Plaza (2024), quien, basado en una encuesta aplicada a la población ecuatoriana, indica que el 68% de los ecuatorianos, considera que la seguridad digital es un factor clave que influye en la decisión realizar compras en línea. Adicionalmente, el estudio indica que el 51% de los usuarios

considera importante que los métodos de pago digitales cuenten con mayores mecanismos de monitoreo, protección y resguardo.

Por otra parte, el 28% de los encuestados consideran que la falta de claridad en la información de un producto incrementa considerablemente el riesgo al realizar una compra en línea. En este sentido, Suárez Nicolalde (2026), sostiene que la veracidad de la información de los productos promocionados en las plataformas comerciales influye proporcionalmente en su decisión de compra de los usuarios a través de la modalidad online. De acuerdo con Curay Ulcuango y Flores Urgilés (2025), sostienen que la seguridad digital no únicamente cumple una función preventiva, sino que está conformada por diversos estándares y protocolos que permiten evaluar el nivel de protección de los sistemas electrónicos.

En relación con las medidas de seguridad electrónica en las plataformas digitales, expertos en ciberseguridad entrevistados en la Universidad Politécnica Salesiana, sostienen que la ciberseguridad debe abordarse bajo un enfoque controlable y alineado con los siguientes estándares: PCI DSS, ISO/IEC 27001 y OWASP. En concordancia, Coronel Suárez y Quirumbay Yagual (2022), concluyen que los protocolos de seguridad permiten garantizar la efectividad de la protección de los entornos digitales, además de facilitar la detección, prevención y recuperación de los sistemas operativos frente a posibles ataques virtuales. Los resultados presentados en la investigación constituyen una base para el desarrollo de conclusiones y recomendaciones.

4. Conclusión

En conclusión, el presente trabajo de titulación aborda la seguridad digital en las compras de productos mediante plataformas digitales, considerando la percepción de confianza y seguridad de los consumidores guayaquileños. A partir de un análisis investigativo, se recopilaron diversos aportes relacionados con la seguridad digital en los sistemas electrónicos, así como informes y estudios de profesionales que destacan su impacto positivo en la protección de informática en el país.

A partir de los resultados obtenidos en el estudio, es posible inferir que la población guayaquileña presenta una percepción moderada respecto a la seguridad digital en las compras realizadas a través de plataformas digitales. Los hallazgos permiten determinar que, si bien los consumidores reconocen la facilidad que ofrecen los medios tecnológicos para la adquisición de productos, aún persiste una preocupación latente vinculada a los ciberataques, tales como fraudes, robos y estafas virtuales. En este sentido, se evidencia que la ciberseguridad constituye un componente necesario en la decisión de compra en línea, influyendo directamente en el nivel de confianza de los usuarios que utilizan el comercio electrónico en el país.

Por otro lado, el artículo académico presenta algunas limitaciones que deben ser consideradas. Para empezar, el estudio se desarrolló exclusivamente en la ciudad de Guayaquil, lo cual restringe la extensión de los hallazgos hacia otras ciudades del país que podrían presentar realidades socioculturales, tecnológicas y económicas distintas en relación con el uso de plataformas digitales y sus medidas de seguridad electrónica.

En cuanto a las futuras líneas de investigación, se recomienda ampliar el alcance geográfico del estudio hacia otras ciudades y regiones del Ecuador, con la finalidad de analizar la percepción de confianza y seguridad de los ciudadanos que utilizan el e-commerce a nivel nacional. Asimismo, se sugiere profundizar en un análisis técnico de los sistemas de ciberseguridad aplicados en las plataformas electrónicas, así como desarrollar estudios relacionados con el impacto de la educación digital y la alfabetización tecnológica en la reducción de los ciberataques. Estas líneas de investigación permitirán fortalecer y complementar los aportes académicos del presente estudio.

Referencias Bibliográficas

Astudillo-Romero, A. E, & Torres-Negrete, A. de las M. (2024). Auditoría digital un mundo interconectado: seguridad financiera y fiscal en empresas de construcción [Digital auditing in an interconnected world: financial and tax security in construction companies]. Revista Multidisciplinaria Perspectivas Investigativas, 4(especial), 152–163. https://www.rperspectivasinvestigativas.org/index.php/multidiscipinaria/article/view/178

Astudillo Torres, MP, & Chevez Ponce, F. (2021). La escala Likert en la medición de las TIC y la Exclusión Social. Cadernos De Educação Tecnologia E Sociedade, 14 (3), 375-383. https://brajets.com/brajets/article/view/701

Aznar-Martínez, B., Casarramona-Basany, A., Grané-Morcillo, J., Lorente-De-Sanz, J., Prats-Fernández, M.- Àngel, & Ballester-Brage, L. (2024). Uso responsable de Internet y seguridad digital: revisión sistemática de programas educativos. Estudios Sobre Educación, 47, 125-152. https://revistas.unav.edu/index.php/estudios-sobre-educacion/article/view/44726

Becerra Molina, E., Jaramillo Calle, Y., & Eliza Flores, M. (2021). El comercio electrónico en tiempos de COVID-19, en el entorno de los negocios de la región 6. Ciencia Digital, 5(4), 94-113. https://doi.org/10.33262/cienciadigital.v5i4.1872

Barahona-Martínez, G. E., Barzola-Plúas, Y. G., & Peñafiel-Muñoz, L. V. (2024). El Derecho a la Protección de Datos y el Avance de las Nuevas Tecnologías en Ecuador: Implicaciones Legales y Éticas. Journal of Economic and Social Science Research, 4(3), 46-64. https://doi.org/10.55813/gaea/jessr/v4/n3/113

Bueno Valero, G., & Haz, L. (2022). Ciberseguridad post Covid-19 y su impacto en las pymes del Ecuador. Pro Sciences: Revista De Producción, Ciencias E Investigación, 6(46), 103–120. https://journalprosciences.com/index.php/ps/article/view/634

Bravo. (2025). Informe Estado Actual de la Ciberseguridad Ecuador [Current State of Cybersecurity Report for Ecuador]. Revista Líder Tecnológica de Ciencias informáticas (It Ahora). 1-60. https://content.bhybrid.com/publication/71dd7ebf/mobile/?p=1

Cedeño Villacís RP. (2022). Ciberseguridad y Ciberdefensa: Perspectiva de la situación actual en el Ecuador. Revista Tecnológica Ciencia Y Educación Edwards Deming, 6 (1). https://doi.org/10.37957/rfd.v6i1.88

Calle-Tenesaca, M. E., & Andrade-Amoroso, R. P. (2024). Ciberseguridad en contabilidad: protegiendo la integridad de los datos financieros en empresas comerciales. Revista Metropolitana

De Ciencias Aplicadas, 7(S2), 87-98. https://remca.umet.edu.ec/index.php/REMCA/article/view/734

Cornejo Ramos, S. A., & Sánchez, D. X. (2023). La protección de datos de carácter personal frente al delito de interceptación ilegal de datos. Código Científico Revista De Investigación, 4(E2), 984–1023. http://revistacodigocientifico.itslosandes.net/index.php/1/article/view/192

Coronel Suárez, I. A., & Quirumbay Yagual, D. I. (2022). Seguridad informática, metodologías, estándares y marco de gestión en un enfoque hacia las aplicaciones web. Revista Científica y Tecnológica UPSE. https://www.revistas.upse.edu.ec/index.php/rctu/article/view/672?utm_source

Curay Ulcuango, F. R., & Flores Urgilés, C. H. (2025). Impacto de la Ley Orgánica de Protección de Datos y la ISO 27001 en la ciberseguridad empresarial ecuatoriana. Religación, 11(49). https://revista.religacion.com/index.php/religacion/article/view/1588

Chiliquinga-Villacis, J. A., & Redrobán-Barreto, W. E. (2025). Derechos del consumidor frente a ventas fraudulentas en el comercio electrónico en Ecuador. MQRInvestigar, 9(2), e563. https://www.investigarmqr.com/2025/index.php/mqr/article/view/563?utm_source

Estrella Murillo, Y. M., Verdezoto Chuquian, L. M., Escobar López, F. M., Ochoa Cárdenas, W. O., & Moreno Vega, L. G. (2024). Uso Eficiente de Herramientas Digitales en el Proceso Enseñanza Aprendizaje en el Sistema Educativo Ecuatoriano. Ciencia Latina Revista Científica Multidisciplinar, 8(6), 2531-2546. https://doi.org/10.37811/cl_rcm.v8i6.15031

Endara Chamorro RE, Méndez Cabrita CM, Villarreal Lima JS, Portilla Paguay RE. Fortalecimiento de la protección de datos personales mediante la creación de un organismo regulador. Salud, Ciencia y Tecnología - Serie de Conferencias [Internet]. 4 de marzo de 2025 Disponible en: https://conferencias.ageditor.ar/index.php/sctconf/article/view/611?utm_source

Fernández Muerza, Alex (2022). Influencia y evolución de Internet en la Comunicación de la Ciencia y sus fuentes. Fonseca, Journal of Communication, 25, 2022, pp. 5-22. 1-18. https://addi.ehu.es/handle/10810/60801

Heredia Pincay, D., & Villarreal Satama, F. (2022). El comercio electrónico y su perspectiva en el mercado ecuatoriano. ComHumanitas: Revista Científica De Comunicación, 13(1), 1-33. https://doi.org/10.31207/rch.v13i1.333

Instituto Nacional de Estadística y Censos. (2025). Tecnologías de la información y comunicación – TICs (julio 2025) [PDF]. Ecuador. https://www.ecuadorencifras.gob.ec/documentos/web-inec/Estadisticas_Sociales/TIC/2025/202507_Tecnologia_de_la_Informacion_y_Comunicacion-TICs.pdf

Infante Plaza, A. A. I. (2024). Estudio de los factores de seguridad respecto a las compras online. Revista Eruditus, 5(3), 43-54. https://revista.uisrael.edu.ec/index.php/re/article/view/1193?utm_source

Juca-Maldonado, F., & Medina-Peña, R. (2023). Ciberdelitos en Ecuador y su impacto social; panorama actual y futuras perspectivas. Portal De La Ciencia, 4(3), 325–337. https://doi.org/10.51247/pdlc.v4i3.394

López-Anchala, K. A. ., & Ordóñez-Parra, Y. L. . (2024). Auditoría y ciberseguridad en el sector comercial: evaluación de resiliencia ante amenazas digitales [Audit and cyber security in the commercial sector: assessing resilience to digital threats]. Revista Multidisciplinaria Perspectivas Investigativas, 4(especial), 14–27. http://www.rperspectivasinvestigativas.org/index.php/multidiscipinaria/article/view/154

López, C. P., Carrillo, J. A., Flores Urgilés, C., & Ormaza Vintimilla, D. (2023). Modelo de madurez de ciberseguridad para infraestructuras críticas caso de estudio: Ecuador. Pro Science: Revista De Producción, Ciencias E Investigación, 7(48), 39–56. https://journalprosciences.com/index.php/ps/article/view/664

Lucero, L. (2023). El rol de la auditoría informática en la era de la protección de datos personales en Ecuador. Technology Rain Journal, 2(2), e17. https://doi.org/10.55204/trj.v2i2.e17

Minaya Macias, M. M, Minaya Macias, R. W, Intriago Navarrete, M. L, & Intriago Navarrete, J. A.. (2023). Normas y estándares en auditoría: una revisión de su utilidad en la seguridad informática. Revista Científica Arbitrada Multidisciplinaria PENTACIENCIAS, 5(4), 584–599. https://doi.org/10.59169/pentaciencias.v5i4.700

Mera Servigón. (2021). Desafíos del comercio electrónico para las PYMES ecuatorianas. Espí-ritu Emprendedor TES, 5(4), 19–39. https://doi.org/10.33970/eetes.v5.n4.2021.285

Medina Romero, M. Ángel, Hurtado Tiza, D. R., Muñoz Murillo, J. P., Ochoa Cervantez, D. O., & Izundegui Ordóñez, G. (2023). Método mixto de investigación: Cuantitativo y cualitativo. Instituto Universitario de Innovación Ciencia y Tecnología Inudi Perú. https://editorial.inudi.edu.pe/index.php/editorialinudi/catalog/book/118

Molina Tenesaca, D. M., Ordoñez Naula, V. A., Farez Arias, M. R., & Carmenate Fuentes, L. P. (2025). Impacto de plataformas digitales en eficiencia y procesos comerciales de exportación de cacao en El Oro. Ciencia Y Educación, 6(10.2), 197 - 210. https://doi.org/10.5281/zenodo.17653637

Moreira Moreira, I. A., Navia Mendoza, M., & Parraga-Alava, J. (2024). El derecho informático y la influencia en los sistemas de información: un análisis bibliográfico bajo la perspectiva jurídica y tecnológica en Ecuador. Revista Tecnológica - ESPOL, 36(1), 162-178. https://doi.org/10.37815/rte.v36n1.1151

Peñarrieta, D., Navia, M., Garcia, E., & Zambrano, D. (2024). Evaluación de la Seguridad de Certificados Digitales en las Plataformas Financieras de Ecuador. Revista Tecnológica - ESPOL, 36(2), 174-189. https://doi.org/10.37815/rte.v36n2.1222

Portilla Paguay, R. E., Menza Ortega, E. J., & Portilla Paguay, M. P. (2025). Delitos informáticos en el Código Orgánico Integral Penal: una revisión sobre acceso no autorizado, fraude digital y ciberseguridad en Ecuador. Pro Sciences: Revista De Producción, Ciencias E Investigación, 9(60), 114–127. https://journalprosciences.com/index.php/ps/article/view/911

Quintero-López, E.. (2020). Plataformas comerciales. Con-Ciencia Boletín Científico De La Escuela Preparatoria No. 3, 7(14), 8–9. Recuperado a partir de https://repository.uaeh.edu.mx/revistas/index.php/prepa3/article/view/6103

Reyes, O., Espinosa, R., & Olvera, R. (2013). Criterios para determinar el Tamaño de Muestra en Estudios Descriptivos. In Congreso Internacional de Investigación de Celaya (México) (Vol. 5, No. 3, pp. 2919-2924). https://www.researchgate.net/profile/Octavio-Reyes-Lopez/publication/331687597_Criterios_para_determinar_el_Tamano_de_Muestra_en_Estudios_Descriptivos/links/5c880965299bf14e7e7820d9/Criterios-para-determinar-el-Tamano-de-Muestra-en-Estudios-Descriptivos.pdf

Ordóñez Córdova, L. A. . (2024). El Marco Legal de los Delitos Cibernéticos en Ecuador. Reincisol., 3(5), 1447–1469. https://www.reincisol.com/ojs/index.php/reincisol/article/view/158

Santamaría-Mendoza, A., Uzcátegui-Sánchez, C., & Vélez-Yaguana, P. (2024). Breve revisión de la literatura del comercio electrónico y sus implicaciones económicas en el Ecuador. Revista Científica Episteme & Praxis, 2(1), 37–49. https://doi.org/10.62451/rep.v2i1.40

Santillán Molina, A. L. (2024). Impacto de centralizar bases de datos en Ecuador con ciberseguridad basada en inteligencia artificial. Universidad Y Sociedad, 16(6), 454–464. Recuperado a partir de https://rus.ucf.edu.cu/index.php/rus/article/view/4786

Silvia Andrade, G. J. S., León, S. D. C., & Gusqui, E. D. M. (2024). La preservación de la privacidad y la salvaguardia de datos personales en el contexto de las redes sociales: un análisis de su impacto en el derecho a la intimidad. Dilemas contemporáneos: Educación, Política y Valores.

https://dilemascontemporaneoseducacionpoliticayvalores.com/index.php/dilemas/article/view/4055

Suárez Nicolalde, C. D. L. Ángeles. (2026). Comportamiento del consumidor y decisión de compra online: un estudio empírico sobre factores determinantes en Quito, Ecuador. Revista Científica Arbitrada Multidisciplinaria PENTACIENCIAS, 7(5), 505–518. https://editorialalema.org/index.php/pentaciencias/article/view/1686

Salazar Larico, P. L. I. S. (2021). Sistema de Seguridad electrónica basada en la norma ISO 27001. INF-FCPN-PGI Revista PGI, 156-159. https://ojs.umsa.bo/index.php/inf_fcpn_pgi/article/view/75

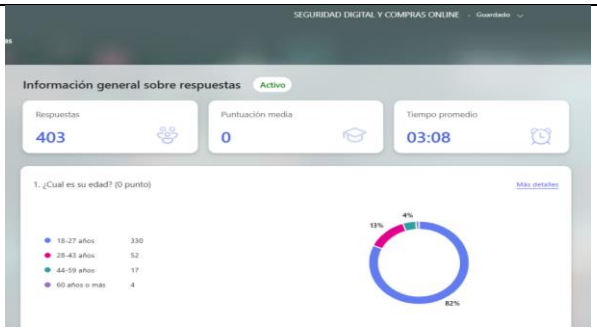
Tayupanta-Guangatal, D. A., Mafla-Sánchez, M. C., Hurtado-Acosta, N., & Alfonso-Gonzáles, I. (2024). Protección de datos personales en era digital [Personal data protection in the digital age]. Verdad Y Derecho. Revista Arbitrada De Ciencias Jurídicas Y Sociales, 3(especial_Ambato), 357-363. https://doi.org/10.62574/6ta6bg70

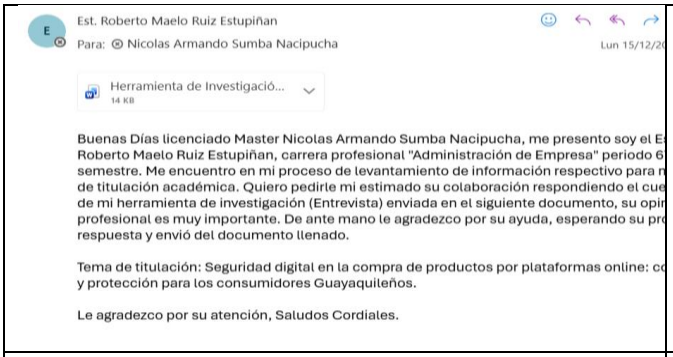
Tunqui Cruz. (2024). Ciberseguridad: Protección de la empresa en la era digital. Revista Maya Administración y Turismo. Vol.6 Núm.2 14-26. https://revistamaya.org/index.php/maya/article/view/1166?utm_source

Veloz-Segura, V. T., Veloz-Segura, E. A., & Tamami-Pachala, J. W. (2025). Ciberseguridad y protección de datos. Revista Científica Arbitrada De Investigación En Comunicación, Marketing Y Empresa REICOMUNICAR. ISSN 2737-6354., 8(16), 168-179. Recuperado a partir de https://reicomunicar.org/index.php/reicomunicar/article/view/452?utm_source

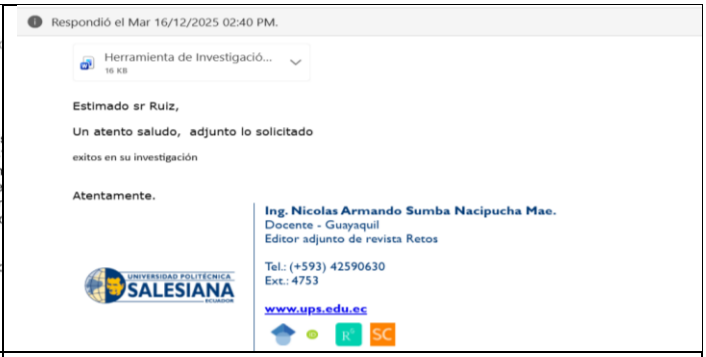
Véliz Intriago, A. K. (2024). Hacia el Futuro Digital: E-commerce y Transformación en el Contexto Ecuatoriano. Ciencia Latina Revista Científica Multidisciplinar, 7(6), 8374-8395. https://ciencialatina.org/index.php/cienciala/article/view/9375?utm_source

Anexos:

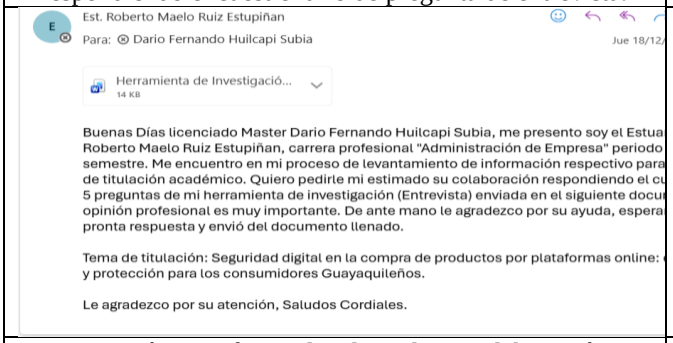
<table>
<tr><td> 
</td><td> 
</td></tr>
<tr><td>Cuestionario de Cuestionario de Pregunta de encuesta en Microsoft Forms.</td><td>Evidencia de numero de respuestas alcanzadas por 403 participantes.</td></tr>
<tr><td>  </td><td>  </td></tr>
<tr><td>Evidencia de Resultados de las preguntas encuestadas</td><td>Evidencia de Resultados de las preguntas encuestadas</td></tr>
<tr><td> 
</td><td> 
</td></tr>
<tr><td>Capturas de finalización de la encuesta por un participante</td><td>Capturas de finalización de la encuesta por un participante</td></tr>
<tr><td> 
</td><td> 
</td></tr>
<tr><td>Invitación a profesional, solicitado su colaboración respondiendo el cuestionario de pregunta de entrevista.</td><td>Respuesta de parte del profesional, evidenciando su participación en la entrevista.</td></tr>
</table>



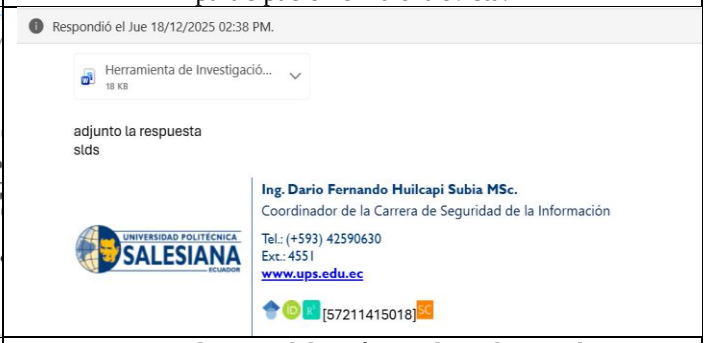
Invitación a profesional, solicitado su colaboración respondiendo el cuestionario de pregunta de entrevista.



Respuesta de parte del profesional, evidenciando su participación en la entrevista.



Invitación a profesional, solicitado su colaboración respondiendo el cuestionario de pregunta de entrevista.



Respuesta de parte del profesional, evidenciando su participación en la entrevista.

Preguntas de Entrevista dirigida a Expertos en ciberseguridad y en sistemas computacionales:

Tabla 7

Entrevista: Mecanismos importante para protección de datos informáticos en las plataformas digitales.

Pregunta 1	Entrevistado 1	Entrevistado 2	Entrevistado 3
¿Cuáles son los principales mecanismos de seguridad digital que, desde su experiencia, deben implementar las plataformas digitales para garantizar la protección de los datos personales y financieros de los consumidores en Guayaquil?	Entre los principales mecanismos de seguridad digital propongo los siguientes: Cifrado de transporte mediante TLS 1.2 (Cifrado de datos utilizando), algoritmos robustos como AES-256; Autenticación multifactor; Desarrollo de aplicaciones bajo estándares seguros como OWASP; En la medida de lo posible uso de token para acceso; Implementación de SIEM	Si se trata de un sitio web, el certificado de seguridad "candadito" que se visualiza junto a la URL del sitio, considero que es fundamental. También definir contraseñas seguras de acceso (exigir a los usuarios), protocolos de seguridad según normativa internacional. Implementar las prácticas de la GDPR (Reglamento General de Protección de Datos) que, aunque rige en Europa se pueden acoger. Si la	La protección de datos informáticos requiere un enfoque de seguridad en profundidad (Defense-in-Depth), implementando múltiples capas de control. Los mecanismos esenciales son: • Cifrado de extremo a extremo (E2EE): Uso de TLS/SSL (versiones robustas como TLS 1.2 o 1.3) para todas las comunicaciones (datos en tránsito) y cifrado con algoritmos fuertes (ej. AES-256) para los datos almacenados en bases de datos. • Autenticación Fuerte: Implementar la Autenticación Multifactor (MFA) o de Dos Factores (2FA) para los usuarios y administradores.

	para detectar incidentes; Implementación de seguridad perimetral; Implementación de estándar iso 27001.	empresa tiene data center en sus oficinas, implementar seguridades como firewall y DMZ.	• Controles de Acceso (RBAC): Aplicar el principio de Mínimo Privilegio. Solo el personal y los sistemas necesarios deben tener acceso a los datos sensibles. Esto se gestiona mediante el Control de Acceso Basado en Roles (Role-Based Access Control - RBAC). • Protección contra Ataques Web: Uso de Firewall, (WAF) para mitigar ataques comunes como Inyección SQL (SQLi) y ripting (XSS).

Tabla 8

Entrevista: Protocolos de ciberseguridad para protecciones de transacciones financieras.

Pregunta 2	Entrevistado 1	Entrevistado 2	Entrevistado 3
¿Qué protocolos o estándares de ciberseguridad considera indispensables para evaluar y proteger las transacciones de pago financieros realizados a través de las plataformas digitales?	Protocolos que se deben aplicar en los sistemas electrónicos: PCI DSS (Payment Card Industry Data Security Standard); TLS (Transport Layer Security); Estándares EMV (Europay, MasterCard, Visa); Cifrado fuerte (AES-256, RSA/ECC para intercambio de claves); ISO/IEC 27001; OWASP; SIEMS; NIST Cybersecurity Framework (CSF) 2.0	Certificado de seguridad SSL para sitios web. Alianza con pasarelas de pago reconocidas para el manejo de pagos digitales como Paymentez, Payphone, PlacetoPay entre otras.	Para las transacciones de pago, es el cumplimiento de estándares internacionales específicos, que deben ser la base para cualquier auditoría y diseño de seguridad: • PCI DSS (Payment Card Industry Data Security Standard): Este es el estándar más indispensable para aquellas plataformas que procesen, almacenen o transmitan datos de tarjetas de crédito (Visa, Mastercard, etc.). • ISO/IEC 27001 (Sistemas de Gestión de la Seguridad de la Información - SGSI): Su implementación asegura que la seguridad sea un proceso continuo, incluyendo la evaluación de riesgo. • OWASP ASVS (Application Security Verification Standard): Este estándar es necesario para evaluar el resguardo de las fuentes y la arquitectura de la aplicación en sí misma. Ofrece una lista de chequeo exhaustiva para verificar si las aplicaciones cumplen con los mejores principios de seguridad en la capa de desarrollo.

Tabla 9

Entrevista: Recomendaciones para fortalecer la seguridad en las plataformas digitales.

Pregunta 3	Entrevistado 1	Entrevistado 2	Entrevistado 3
¿Qué recomendaciones técnicas propondría para fortalecer los	Implementar cifrado fuerte de datos (TLS 1.2/1.3) y en reposo (AES-256); Exigir autenticación multifactor (MFA) en todos los accesos	Implementar certificado de seguridad para sitios web SSL. Si el sitio web es hecho con Wordpress u otro gestor de páginas web,	Las recomendaciones deben estar enfocadas tanto en la prevención como en la detección y respuesta: • Integrar DevSecOps en el ciclo de desarrollo: Implementar pruebas de

sistemas de seguridad de las plataformas digitales?	críticos; Aplicar control de accesos por roles (RBAC) y el principio de mínimo privilegio; Cumplir con PCI DSS en plataformas que gestionen pagos electrónicos; Adoptar el NIST Cybersecurity Framework (CSF) como modelo de gestión de seguridad; Usar Tokenización para proteger datos financieros sensibles; Implementar monitoreo continuo y SIEM para detección temprana de amenazas.	eliminar cuentas por defecto, instaurar contraseñas seguras. Desinstalar plugins que no se usen o desactualizados mejor instalar un plugin de seguridad actualizados.	seguridad automatizadas (SAST/DAST - Static/Dynamic Application Security Testing) directamente en las fases de desarrollo y despliegue (CI/CD) para identificar vulnerabilidades antes de que el código llegue a los servidores. • Segmentación de Red y Microsegmentación: Separar la red de procesamiento de pagos y la base de datos de datos sensibles del resto de la infraestructura (segmentación). • Gestión Proactiva de Parches y Vulnerabilidades: Establecer un programa riguroso de Patch Management para aplicar inmediatamente las correcciones de resguardo a sistemas operativos. • Adoptar Principios de Cero Confianza (Zero Trust): Asumir que ningún usuario, dispositivo o red (interno o externo) es de confianza por defecto. Toda solicitud de acceso debe ser verificada y autenticada continuamente.

Tabla 10

Entrevista: Evaluación de la efectividad de los mecanismos de ciberseguridad por expertos.

Pregunta 4	Entrevistado 1	Entrevistado 2	Entrevistado 3
Desde su punto de vista profesional ¿Cómo evalúa la efectividad de los mecanismos de seguridad digital que utilizan las plataformas digitales en la actualidad?	Como usuario habitual de plataformas transaccionales en línea de empresas, comercios y bancas del Ecuador, considero que los mecanismos de seguridad digital actuales son aceptables pero desiguales: el sector bancario muestra avances claros mediante autenticación multifactor, alertas en tiempo real y controles antifraude, lo que genera confianza; sin embargo, muchos comercios y plataformas de servicios aún presentan controles básicos o poco consistentes.	En primer lugar, reviso que el sitio web disponga de SSL (candadito). La pasarela de pago debe ser una que tenga trayectoria en el mercado como Paymentez, Placetopay. Y para medir la efectividad, deberían ser cero o cercanos a cero los eventos relacionados con robo de información, acceso no autorizado, caídas de servicio propiciadas por ataques DDoS (denegación de servicio).	La efectividad es, en general, variada y dependiente del sector y la inversión. • En las plataformas maduras (Banca, E-commerce): Tienden a tener una alta efectividad. Esto se debe a que están obligadas a cumplir con estándares rigurosos (como PCI DSS y regulaciones locales), invierten constantemente en tecnología de punta (WAF - Web Application Firewall, SIEM - Security Information and Event Management (Gestión de la Información y Eventos de Seguridad, Tokenización) • En las plataformas PYME o emergentes: Suelen tener una efectividad media a baja. A menudo se enfocan en la funcionalidad y la rapidez, implementando como un requisito secundario. Esto se traduce en configuraciones predeterminadas no seguras, falta de MFA (Autenticación Multifactor), cifrado débil en tránsito y ausencia de un WAF (Web Application Firewall).

Tabla 11

Entrevista: Medidas de ciberseguridad en la protección de sistemas electrónicos.

Pregunta 5	Entrevistado 1	Entrevistado 2	Entrevistado 3
Desde su experiencia, ¿en qué medida los sistemas de ciberseguridad ayudan a las plataformas de comercialización en línea en evaluar su rendimiento de la protección sus sistemas operativos, contribuyen a la reducción de fraudes y estafas en el país?	Desde mi punto de vista, los sistemas de ciberseguridad contribuyen en alta medida a que las plataformas de comercialización en línea evalúen el rendimiento de la protección de sus sistemas operativos y, al mismo tiempo, reduzcan fraudes y estafas en el país. En primer lugar, permiten medir objetivamente la efectividad de los controles de seguridad mediante indicadores como intentos de acceso no autorizado, transacciones bloqueadas, tiempos de detección y respuesta, y cumplimiento de estándares (NIST, ISO 27001, PCI DSS), lo que facilita la mejora continua de los sistemas. En segundo lugar, mecanismos como el monitoreo en tiempo real, la autenticación multifactor, la detección de anomalías y los motores antifraude reducen de forma directa la probabilidad de suplantación de identidad.	Considero que son fundamentales para mitigar los casos de fraudes y estafas, las empresas deberían invertir recursos y tiempo sobre todo si se dispone de una e-commerce. Los datos y la confidencialidad de las personas que transaccionan en dicho e-commerce es fundamental.	Los sistemas de ciberseguridad son necesarios y tienen un impacto directo y cuantificable en la reducción de fraudes y estafas: • Rendimiento de la Protección (Sistemas Operativos): Los sistemas de ciberseguridad (como las herramientas de Gestión de Vulnerabilidades, Antivirus/EDR y Análisis de Registros - SIEM) evalúan el rendimiento de la protección al ofrecer una vista en tiempo real del posture de seguridad. Miden la "higiene cibernética" (ej. porcentaje de máquinas con parches aplicados, detección de malware en endpoints). • Contribución a la Reducción de Fraudes y Estafas: En mecanismos de Detección de Fraude Transaccional, el uso de sistemas antifraude basados en machine learning que analizan el comportamiento del usuario (ubicación, velocidad de compra, historial, device fingerprinting) es el principal contribuyente. Estos sistemas pueden detener transacciones fraudulentas en milésimas de segundo. En la protección de la confidencialidad, al prevenir las filtraciones de datos (mediante cifrado y segmentación).

Tabla 12

Términos mencionados en el trabajo sobre la seguridad digital en los medios electrónicos.

Términos utilizados	Abreviación	Definición
TLS/SSL	(Seguridad de la capa de transporte/Capa de sockets seguros)	Protocolos criptográficos que protegen la comunicación entre cliente y servidor.
AES	Estándar de cifrado avanzado	Estándar de cifrado simétrico para resguardo de los almacenamientos informáticos.
SIEM	Gestión de información de seguridad	Mecanismo que analiza eventos de seguridad para detectar incidentes en tiempo real.
ISO/IEC	Organización Internacional de Normalización / Comisión Electrotécnica Internacional	Organismos internacionales que desarrollan normas técnicas para resguardo de los medios tecnológicos.
OWASP	Proyecto de seguridad de aplicaciones abierto a nivel mundial	Organización que promueve buenas prácticas y guías para la seguridad de aplicaciones web.

PCI DSS	Estándar de protección de datos de la industria de tarjetas de pago	Estándar de seguridad para organizaciones financieras.
NIST	Instituto Nacional de Estándares y Tecnología	Instituto que desarrolla marcos y guías de ciberseguridad utilizados a nivel internacional.
DevSecOps	Mecanismo de Desarrollo, Seguridad y Operaciones electrónicas	Protocolos de operaciones de protecciones y resguardo de los sistemas operativos.
SAST/DAST	Pruebas de seguridad de aplicaciones estáticas / Pruebas de seguridad de aplicaciones dinámicas	Métodos de prueba que permiten identificar vulnerabilidades en aplicaciones, tanto en el código como en ejecución.
MFA	Autenticación multifactor	Mecanismo de autenticación que utiliza dos o más factores de verificación para acceder a sistemas.
WAF	Cortafuegos de aplicaciones web	Firewalls especializados en la protección de filtración de datos electrónicos.
FIREWALL	cortafuegos	Medida de seguridad de control acceso para resguardo de los medios tecnológicos.