UNIVERSIDAD POLITÉCNICA SALESIANA ECUADOR

POSGRADOS

Maestría en

COMERCIO EXTERIOR Y GESTIÓN LOGÍSTICA

RPC-SO-33-NO.762-2021

Opción de Titulación:

PROYECTO DE TITULACIÓN CON COMPONENTES DE INVESTIGACIÓN APLICADA Y/O DE DESARROLLO.

Tema:

CIBERSEGURIDAD EN EL COMERCIO ELECTRONICO Y SU CONTINUIDAD OPERATIVA EN ORGANIZACIONES ECUATORIANAS

Autor(es)

GENESIS DENNIS MOSQUERA QUIMIS

JAIR STEEVE TAMAYO CHICAIZA

Director:

Stella Paola Delgado Figueroa

GUAYAQUIL – Ecuador

2025

Autor(es):

Genesis Dennis Mosquera Quimis
Ing. Contabilidad y Auditoría - CPA
Candidata a Magíster en Comercio Exterior y Gestión Logística por la Universidad Politécnica Salesiana – Sede Guayaquil.
gmosqueraq@est.ups.edu.ec

Autor(es):

Jair Steeve Tamayo Chicaiza
Ing. en Comercio Exterior
Candidato a Magíster en Comercio Exterior y Gestión logística por la Universidad Politécnica Salesiana – Sede Guayaquil.
jtamayoc2@est.ups.edu.ec

Dirigido por:

Stella Paola Delgado Figueroa
Economista
Magister en Negocios Internacionales y Gestión en Comercio Exterior
sdelgadof@ups.edu.ec

Todos los derechos reservados.

Queda prohibida, salvo excepción prevista en la Ley, cualquier forma de reproducción, distribución, comunicación pública y transformación de esta obra para fines comerciales, sin contar con autorización de los titulares de propiedad intelectual. La infracción de los derechos mencionados puede ser constitutiva de delito contra la propiedad intelectual. Se permite la libre difusión de este texto con fines académicos investigativos por cualquier medio, con la debida notificación a los autores.

DERECHOS RESERVADOS
2025 © Universidad Politécnica Salesiana
GUAYAQUIL - ECUADOR - SUDAMÉRICA
GENESIS DENNIS MOSQUERA QUIMIS
JAIR STEVEN TAMAYO CHICAIZA
CIBERSEGURIDAD EN EL COMERCIO ELECTRONICO Y SU CONTINIUDAD OPERATIVA EN ORGANIZACIONES ECUA TORIANAS

AGRADECIMIENTO

Expreso mis más sinceros agradecimientos a todas aquellas personas que de una u otra forma han contribuido a la culminación de esta nueva etapa de mi vida.

Agradezco a Dios y a mis padres por haber forjado los cimientos de mi formación, por su apoyo, dedicación y amor incondicional.

A mi directora del trabajo de titulación por su ayuda incondicional en la guía de elaboración de este proyecto y conocimientos prestados durante esta etapa.

A la Universidad Politécnica Salesiana por haberme facilitado llegar a este logro y permitirme culminar otra etapa significativa en mi desarrollo profesional.

A todos, expreso mis constantes agradecimientos.

Tabla de Contenido

Ciberseguridad en el comercio electrónico y su continuidad en organizaciones ecuatorianas

Autor(es):

GENESIS DENNIS MOSQUERA QUIMIS
JAIR STEVEN TAMAYO CHICAIZA

Resumen

La evolución de la ciberseguridad en el comercio electrónico abarca un conjunto de estrategias, tecnologías y procesos que tienen como finalidad proteger datos importantes, redes sociales y dispositivos móviles contra daños, ataques o accesos no autorizados brindando mayor protección, confianza, integridad y fiabilidad en el manejo de los datos de personas naturales o jurídicas en el entorno virtual. Con la llegada de la era digital, los avances tecnológicos y la inteligencia artificial han generado múltiples vulnerabilidades cibernéticas que poner en peligro los sistemas informáticos, los activos de las empresas incluida la información confidencial de sus clientes. Por esta razón, este estudio examinará el impacto de estos ataques y las medidas que han adoptado las organizaciones ecuatorianas, utilizando un enfoque descriptivo y exploratorio a través de la recopilación de información basada en artículos científicos, normativas internacionales y análisis estadísticos. En este contexto, los hallazgos enfatizan el fortaleciendo de la seguridad cibernética en las empresas analizadas a través de sistemas de salvaguarda y la incorporación de soluciones tecnológicas. Sin embargo, existen falencias en la formación del personal y en la implementación de normativas legales. En conclusión, es de vital importancia que las organizaciones adopten regulaciones de seguridad nacional como la Ley Orgánica de Protección de Datos Personales (LOPDP) y obtengan certificaciones bajo normas internacionales como la ISO/IEC 27001 para hacer frente a un entorno digital que está en constante cambio, garantizando la continuidad operativa, así como la resiliencia digital y la confianza en el contexto internacional.

Palabras claves:

Seguridad, comercio, protección, datos, continuidad, resiliencia

Abstract

The evolution of cybersecurity in e-commerce encompasses a set of strategies, technologies, and processes aimed at protecting important data, social networks, and mobile devices from harm, attacks, or unauthorized access, providing greater protection, trust, integrity, and reliability in the handling of data belonging to individuals or legal entities in the virtual environment. With the arrival of the digital age, technological advances and artificial intelligence have generated multiple cyber vulnerabilities that endanger computer systems, corporate assets, and customers' confidential information. For this reason, this study will examine the impact of these attacks and the measures adopted by Ecuadorian organizations, using a descriptive and exploratory approach through the collection of information based on scientific articles, international regulations, and statistical analysis. In this context, the findings emphasize the strengthening of cybersecurity in the analyzed companies through safeguard systems and the incorporation of technological solutions. However, there are gaps in staff training and the implementation of legal regulations. In conclusion, it is vitally important for organizations to adopt national security regulations such as the Organic Law on Personal Data Protection (LOPDP) and obtain certifications under international standards such as ISO/IEC 27001 to address a constantly changing digital environment, ensuring operational continuity, as well as digital resilience and trust in the international context.

Keywords:

Security, commerce, protection, data, continuity, resilience

1. Introducción

Después de concluir la Segunda Guerra Mundial, la expansión del capitalismo a través de mercados e instituciones internacionales impulsó el proceso de globalización, también conocido como hiperglobalización. El Informe de UNCTAD (2019), el desarrollo de Internet y las tecnologías digitales ha sido uno de los factores fundamentales de la transformación económica mundial, mejorando la economía mundial y promoviendo un dinamismo comercial, cultural y social. Es de conocimiento general que el ciberespacio permite la interconexión y facilita la comunicación instantánea entre personas, empresas y gobiernos de distintas partes del mundo. Sin embargo, el Internet es el presente; así lo define Castells (2001), quien incluso lo considera un medio de comunicación interactiva de carácter social. Con los avances de la hiperglobalización se logró el desarrollo de las Tecnologías de la Información y la Comunicación (TIC), la digitalización y diversas formas de comercializar productos o servicios. En este sentido, San Román (2019) señala que la globalización, junto con los avances tecnológicos, ha transformado la perspectiva del comercio tradicional, cumpliendo una función clave en el crecimiento económico, al reinventar las relaciones comerciales. La incorporación de tecnologías digitales en las organizaciones ha facilitado la sostenibilidad de la competencia entre las empresas, con el fin de mantenerse actualizadas y alcanzar sus metas (Medina et al., 2019).

La adaptación del comercio con el internet ha creado más oportunidades en los mercados locales e internacionales para realizar transacciones físicas o virtuales, sin considerar la ubicación del individuo. De acuerdo con Barzola et al. (2019), el E-Commerce se define como la transacción de productos o servicios a través de internet o plataformas digitales, que puede realizarse desde cualquier parte del mundo, sin considerar la diferencia horaria. Cuando las empresas digitalizan sus productos en la web, inician con la difusión de su actividad comercial en redes sociales, generando contenidos publicitarios informativos. Para Grillo (2021), el intercambio de bienes y servicios entre organizaciones (públicas, privadas o mixtas) y personas jurídicas o naturales implica relacionarse en un manejo de infraestructura de red o las TIC, considerando que los mismos deben adaptarse a la era digital. En contraste, Hashemi-Pour y Lutkevich (2023) definen el comercio en línea como “la adquisición y venta de productos y servicios, o la transferencia de dinero o información, por medio de una red electrónica, principalmente Internet”.

Por consiguiente, se demuestra que el comercio electrónico es un recurso estratégico, eficaz e indispensable en las transacciones de organizacionales, de acuerdo con la clase de negocio electrónico que manejen. Herrero (2021) menciona diversas tipologías de comercio electrónico, tales como: *Business to Business* (B2B),

Business to Consumer (B2C), *Consumer to Business* (C2B), *Consumer to Consumer* (C2C), *Business to Government* (B2G), *Consumer to Government* (C2G), *Government to Business* (G2B), y *Government to Consumer* (G2C), debido a la implementación del internet, redes sociales y aplicaciones digitales. Este tipo de mercadeo realizado mediante plataformas digitales experimentó un crecimiento significante a partir de del año 2010, no obstante, con la llegada de la pandemia de Covid-19, se implementaron medidas de bioseguridad alrededor del mundo de manera obligatoria, como el confinamiento, aquel suceso no detuvo la compra y venta por parte de empresas y consumidores.

Por otro lado, una de las consecuencias que se han generado en la web, al comprar o vender bienes tangibles o intangibles, son la divulgación de datos, ataques cibernéticos, malwares, entre otros. Esta idea es complementada por Moreno y Velázquez (2019) quienes destacan que las vulnerabilidades en el comercio electrónico ponen en riesgo la información personal y datos sensibles de los clientes y de la empresa, afectando la confianza de los consumidores en plataformas digitales. Por tal motivo, Valarezo (2020) indica que la ciberseguridad es uno de los pilares fundamentales al momento de realizar compras o ventas a través de plataformas digitales, ya que garantiza la salvaguarda de la información personal y financiera de los usuarios.

Con la expansión progresiva de Internet, las empresas han ido migrando de un modelo tradicional de comercio hacia formatos digitales. Según Shopify (Lin, 2024), las ventas mundiales de comercio electrónico llegaron a unos 6,09 billones de dólares, reflejando un crecimiento del 8,4 % en comparación con 2023. Este aumento no solo muestra la amplia adopción de plataformas de compra en línea, sino también la consolidación de los pagos digitales y el comercio móvil. El comercio electrónico continúa su expansión en América Latina. En 2024, las ventas electrónicas al por menor en la región sobrepasaron los 180 000 millones de dólares y se espera un aumento continuo que llegará a 250 000 millones para 2028 (eMarketer, 2024).

Para concluir, en relación al panorama de ataques cibernéticos para la región según Kapersky (2023), luego de la pandemia y el surgimiento de herramientas con inteligencia artificial se evidenció un aumento significativo del 617% de estafas en internet para el año 2023 en comparación del 2022, donde el ataque cibernético con mayor frecuencia era el phishing y troyanos bancarios. Los países latinoamericanos con ataques en la web son Brasil con 134 millones intentos de ataque, México con 43 millones, Perú con 31,5 millones, Colombia con 30,9 millones, Ecuador con 12,2 millones, Chile con 10,5 millones y Argentina con 9,4 millones.

2. Determinación del Problema

En Ecuador, el comercio digital muestra un notable aumento. La Cámara de Comercio Electrónico de Ecuador (2024) estima ventas digitales en torno a los 2 000 millones de USD anuales, lo que ejemplifica una transición lenta pero sostenida hacia entornos de negocio más digitales. Sin embargo, este aumento de las transacciones digitales, trae consigo un ascenso proporcional en los riesgos e incursiones a la que están expuestas las organizaciones. Como enfatiza Ramos-Secaira (2023), la seguridad cibernética en las empresas del Ecuador es un asunto de mayor relevancia que requiere atención inmediata. Los desafíos son numerosos y complejos, pero mediante un enfoque sistemático y bien informado, es posible desarrollar estrategias que mejoren la protección de los sistemas y datos corporativos.

En este marco, se reconoce como problema central la permanente exposición de los sistemas informáticos a múltiples tipos de ciberataques como el robo de información, ataques de ransomware, suplantaciones de identidad y violaciones a la seguridad. Esto resalta la necesidad de aplicar controles tecnológicos, estrategias integrales de seguridad digital y fortalecer las competencias del recurso humano. Aunque en el país existen los marcos regulatorios, como la *Ley Orgánica de Protección de Datos Personales* (Asamblea Nacional del Ecuador, 2021), y *la Estrategia Nacional de Ciberseguridad* (Ministerio de Telecomunicaciones y de la Sociedad de la Información [MINTEL], 2022), que tienen como objetivo proteger la privacidad y asegurar un manejo responsable de los datos por entidades tanto públicas como privadas, persisten retos importantes en su implementación, cumplimiento y articulación con los procesos operativos del sector empresarial.

3. Justificación

El presente estudio resulta pertinente debido al papel fundamental de la relación entre la ciberseguridad y la continuidad operativa en las organizaciones ecuatorianas que operan en el sector del comercio en línea. El crecimiento de las transacciones digitales y la integración de tecnologías en los sistemas empresariales con la finalidad de expandir el mercado, han creado una alerta a nivel mundial sobre los protocolos que se están utilizando en la seguridad web para evitar la divulgación de datos. Si bien es cierto, la ciberseguridad no solo es salvaguardar los datos sensibles de empresas y usuarios, sino también aumentar la confianza en plataformas de comercio digital. Las empresas necesitan invertir en expertos en seguridad de las Tecnologías de la Información y la Comunicación (TICS) y llevar a cabo análisis continuos de sus defensas cibernéticas, ya que el avance tecnológico las expone a ataques, poniendo en riesgo la confidencialidad, integridad y

disponibilidad de la información.

Los beneficiarios de esta investigación abarcan a todos los usuarios de plataformas de comercio electrónico, ya que muestra la relevancia de contar con un protocolo de seguridad para la continuidad de las actividades comerciales. Además, proporciona información valiosa para investigadores y expertos de diversas áreas empresariales, permitiéndoles obtener conclusiones sobre la aplicación de estrategias de ciberseguridad que minimice el impacto de divulgación de datos empresariales en la web y fortalezca la continuidad operativa de la organización.

4. Objetivos

Objetivo General

Analizar la relación entre la ciberseguridad y la continuidad operativa en las organizaciones ecuatorianas que operan en el ámbito del comercio electrónico.

Objetivos Específicos

1. Identificar las principales amenazas cibernéticas que enfrentan las organizaciones ecuatorianas en el comercio electrónico.

2. Describir las estrategias y tecnologías de ciberseguridad implementadas por las organizaciones ecuatorianas para proteger sus operaciones en el comercio electrónico.

3. Determinar la relación entre la efectividad de las medidas de ciberseguridad y la capacidad de las organizaciones ecuatorianas para mantener la continuidad operativa en el comercio electrónico.

5. Marco teórico referencial

5.1 Comercio Electrónico en el Ecuador

La convergencia entre el comercio y la tecnología ha fortalecido la competitividad en los niveles nacional e internacional, promovida por la implementación de las TIC. Estas tecnologías se consolidan como actores fundamentales en la configuración de la nueva etapa de la globalización, denominada comúnmente como la Era del Siglo XXI. De acuerdo con la ideología de González y Sanz (2020) la integración de las TIC en el mercado global ha favorecido al sector de empresas multinacionales, debido a la reducción de costes de transacciones, brechas de comunicación y velocidad en

los procesos exportación de pequeñas y medianas empresas (Pymes). La adopción de las TIC ha redefinido las reglas dentro del comercio internacional, facilitando la interconexión entre diversos países, y a su vez exigir nuevas estrategias de operatividad para la continuidad de sus procesos con el objetivo de obtener beneficios de la revolución tecnológica. Al unificar el comercio tradicional y las ciencias aplicadas han dado como resultado la economía digital (E-Commerce).

Según Robayo-Botiva, D. M. (2020) el E-Commerce, es el resultado de las compras de bienes o servicios por internet debido a que se utilizan medios de pago digitales. Adicionalmente, Paz (2021) enfatiza que el comercio electrónico es un elemento importante que impulsa el dinamismo comercial, no obstante, se requiere que la infraestructura tecnológica de las empresas facilite y agilice los procesos de compraventa, tomando en consideración la logística y su fiabilidad en los medios de pago.

En esta misma línea, de acuerdo con un informe de la Cámara Ecuatoriana de Comercio Electrónico (CECE) en el 2024, la región ecuatoriana a pesar de no ser un país del primer mundo ha logrado posicionarse en el quinto lugar entre los países de Suramérica por uso del servicio de internet, con un 84% con un crecimiento pronosticado del 4%. Así mismo, el informe destaca que, en el ranking mundial del año 2024, Ecuador ocupa el puesto 107 en acceso a internet y conectividad, mientras que en América del Sur se ubica en la séptima posición. Por otra parte, esta misma organización reporta que las transacciones digitales en Ecuador han crecido un 206% entre 2018 y 2023, dando como resultado una tasa de crecimiento anual del 18%, lo que representaría 2.844 millones de dólares (USD). En el ámbito financiero, se logró evidenciar un crecimiento aproximado del 5% representando 20.746 millones de dólares (USD) a comparación del año pasado, donde el monto por transacciones digitales era de 19.807 millones de dólares (USD).

Finalmente, la CECE expresa a través de su investigación que el segmento de retailers ha crecido un 10% a comparación del año 2022. Para el año 2024, se espera observar una proyección estimada del 8% que representaría $ 2,894 millones USD. Durante el año 2023, el país reflejó un monto de ventas en comercio electrónico a nivel nacional de 2.073 millones de dólares (USD), un 3% a diferencia del año 2022 donde se efectuaron ventas de 2.138 millones de dólares (USD).

5.2 Ciberseguridad en el Comercio Electrónico

Con la llegada del internet, las empresas indiferentes a su tamaño iban transformando sus operaciones, es decir, pasando del comercio tradicional al comercio electrónico, ya sea, combinando sus métodos de ventas a lo virtual o combinando lo tradicional con lo digital. En la actualidad, según un informe de

Statista elaborado por Orus (2024) el intercambio comercial cibernético generó 5.8 billones de dólares (USD) hasta el 2023, y se estima que para finales del año 2024 el incremento sea de 6.8 billones de dólares (USD), es decir un crecimiento positivo aproximado del 10%. Adicionalmente, el autor menciona que el 90% de la población mundial ha realizado compras a través de plataformas de tiendas virtuales en el ciberespacio, facturando un total aproximado de 4.2 billones de dólares (USD). De igual manera la vinculación de la tecnología frente a la economía y el ámbito global ha beneficiado significativamente a diversos sectores empresariales del mercado, no solo por reducir tiempos de entrega o comunicación entre diversos países, sino también en aspectos como la traducción de documentos, actualización de nuevos conocimientos, entre otros. Para Becerril y Ortigoza (2018), la interconectividad ha logrado superar barreras comerciales previamente impensables. No obstante, los autores enfatizan la importancia de poseer un protocolo de seguridad, porque el internet aún es una tecnología joven que puede ser manipulada para diversos fines.

Becerril (2019) destaca que la implementación de ciberseguridad en los sistemas integrados de las organizaciones, ayudan a reducir el riesgo de hurto de información, mediante la adopción de métodos de seguridad informática. Además, recalca que la digitalización y el almacenamiento de información en un sistema integrado, han dejado de ser una opción, transformándose en prioridad y necesidad, ya que facilita y optimiza las actividades organizacionales. Por otra parte, Diego et al. (2020) subrayan la importancia de proteger los ordenadores, servidores, y dispositivos con acceso a internet, debido a que, si el usuario no cuenta con un método de seguridad contra ciberataques, se verá expuestos a ser víctimas de *phishing*, *malwares*, hurto de datos, suplantación de datos, entre otros. Para reducir estos riesgos, se sugiere cifrar datos, así como la práctica de programas antivirus, que sean confiables y verificados como McAfee o Kaspersky, autenticación multifactorial, entre otros.

Moreno y Velázquez (2019) enfatizan que las brechas de seguridad en el comercio electrónico, ponen en riesgo la información personal de los clientes y los datos clave de la empresa, afectando la confianza del consumidor en plataformas digitales. La implicación de las empresas en nuevas amenazas cibernéticas es una brecha que afectan los datos de la organización y sus clientes.

Por tal motivo, la ciberseguridad es uno de los pilares fundamentales a considerar al momento de practicar la compra o venta en aplicaciones o plataformas digitales. Meyer (2020), señala que el avance de la digitalización ha generado nuevas vulnerabilidades, tales como hackers o programas maliciosos, lo cual abre un camino a la necesidad de fortalecer las estrategias de protección en el ámbito digital. Adicionalmente, Bhargava (2020), informa que más del 60% de las pequeñas

y medianas empresas que sufren ataques cibernéticos significativas en su operación, lo que en muchos casos conlleva la incapacidad de recuperación total. Lo cual da como resultado, la inversión en sistemas operativos como firewalls, sistemas de detección de intrusos, encriptación de datos y formación orientada a empleados de las empresas para resguardar la información de las partes involucradas.

Un informe citado por IT Ahora (2024) sobre ataques cibernéticos en América Latina registró una cifra récord de 3.9 millones de intentos de ciberataque, superando significativamente las cifras del año 2023. Los países más afectados incluyen Brasil, con 1.8 millones de intentos bloqueados; Ecuador, con 402 mil; México, con 395 mil; y Colombia, con 203 mil. Estos datos posicionan a Ecuador en el top 3 de los países con mayor exposición a amenazas cibernéticas en la región. En esta misma línea, Chevalier (2024), indica que el crecimiento del comercio electrónico en América Latina sigue en aumento, ya que para 2023 se registraron ventas de 117.000 millones de dólares (USD).

En virtud de lo expuesto, esta investigación propone analizar la relación entre la ciberseguridad y la continuidad operativa en las organizaciones ecuatorianas que desarrollan sus actividades en el entorno del comercio electrónico.

5.3 Relación entre Ciberseguridad y Continuidad operativa

Al incorporar tecnología para optimizar procesos dentro de la continuidad operativa de la organización, se debe tomar en cuenta que la información sensible se puede encontrar en situación de riesgo, ya que podría ser divulgada ante la competencia dando como resultado el robo de ideas. Es por esto que Chinchilla (2021), en su artículo sobre la ciberseguridad enfatiza que la nueva era tecnológica ha presentado nuevas oportunidades para la sociedad como la adopción de las tecnologías de la información y las comunicaciones (TIC), la cual ha redefinido las reglas dentro del comercio internacional, facilitando la interconexión entre diversos países, y a su vez exigir nuevas estrategias de operatividad para la continuidad de sus procesos con el objetivo de obtener beneficios de la revolución tecnológica. A su vez, en este mismo sentido menciona el dinamismo que debe poseer la organización y la correcta práctica de protocolos de seguridad informática, ya que señala que es muy fácil que una persona ajena a la empresa pueda controlar un servidor y robar datos para realizar transacciones.

La relación entre ciberseguridad y continuidad operativa es uno de los pilares claves para tener éxito en el mundo digital organizacional. Uno de los beneficios que nos otorga la ciberseguridad es el fortalecer las infraestructuras digitales con el objetivo de minimizar los riesgos de hurto o divulgación de información confidencial. Álvarez

y Díez (2024) enfatizan que “la ciberseguridad es crucial ya que los hackers son más profesionales y, sin duda, utilizan los avances de estas empresas para mejorar su propia eficiencia y productividad sin precedentes” (p.20).

En el entorno organizacional, no se trata de quién posee la ciberseguridad más moderna, sino más bien evolucionar en su giro de negocio y poseer buenas prácticas de seguridad. Los autores dan a entender que la continuidad operatividad de los negocios es el resultado de asumir riesgos en sus inversiones tecnológicas, porque el mundo se ha mal acostumbrado a invertir sus empresas con la finalidad de lograr reconocimiento en el mercado y generar sus ingresos esperados, pero dejando de lado muchas veces el cuidar su información de los hackers. (Calle García et al., 2024) Resalta la agilidad que tienen los ciberdelincuentes, ya que se encuentran diariamente innovando y desarrollando nuevas metodologías para sustraer y comprometer la seguridad de los datos personales u organizacionales.

Por otro lado, Morales Sáenz et al. (2024) señala que la estrategia de ciberseguridad no solo salvaguarda los datos críticos, sino también impulsa a la sostenibilidad económica y social para minimizar interrupciones operativas y garantizar la protección de información sensible. Uno de los ejemplos más recientes, la pandemia de Covid-19 reveló la urgencia de unificar sistemas de seguridad digitales en las organizaciones. Durante este período, la mayoría de las empresas enfrentaron amenazas multifacéticas en la privacidad de sus datos, según la perspectiva de Fezzey et al. (2023), porque el ser humano al encontrarse en una emergencia sanitaria y querer adquirir productos del internet, ya sea para abastecerse de alimentos o medicinas, en muchos casos al ingresar sus datos para realizar el pago de los productos, su información podía ser vulnerada y manipulada, es decir, la persona era víctima de ciberdelincuencia. Es por esto por lo que el mismo autor enfatiza en que los comercios deben tener planes integrales que aborden riesgos complejos frente a los ciberataques y otras crisis de cualquier aspecto.

6. Materiales y Metodología

Esta investigación utilizará un enfoque mixto (cualitativo y cuantitativo) para una comprensión profunda de las ciber amenazas y las tácticas de ciberseguridad, además de evaluar la efectividad de estas en la continuidad operativa. La investigación tendrá un enfoque exploratorio, descriptivo y correlacional. El estudio exploratorio y descriptivo ayudará a identificar y describir las amenazas cibernéticas y las tácticas de ciberseguridad en el comercio electrónico ecuatoriano. El aspecto correlacional se centrará en establecer la conexión entre la eficacia de las acciones de ciberseguridad y la habilidad de las organizaciones para mantener la continuidad operativa.

Para lograr el primer objetivo, identificar las principales amenazas cibernéticas que enfrentan las organizaciones ecuatorianas en el comercio electrónico, se realizará una investigación cualitativa y descriptiva exploratoria por medio de la obtención de información de fuentes secundarias fiables, incluyendo artículos académicos, informes científicos y publicaciones de entidades nacionales, como la Cámara Ecuatoriana de Comercio Electrónico (CECE), la Ley Orgánica de Protección de Datos Personales y el Ministerio de Telecomunicaciones. Los datos obtenidos serán analizados utilizando análisis de contenido, categorizando las amenazas cibernéticas más recurrentes.

Por consiguiente, el segundo objetivo se enfoca en describir las estrategias y tecnologías de ciberseguridad implementadas por las organizaciones ecuatorianas para proteger sus operaciones en el comercio electrónico. Para ello, se realizará una investigación descriptiva mixta mediante entrevistas semiestructuradas, dirigidas a compañías ecuatorianas que operan en el sector del comercio digital, de las que se elegirá una muestra representativa de organizaciones mediante un muestreo estratificado. El tamaño de la muestra es no probabilístico, compuesto por 8 empresas para un total de población con presencia en internet del 79,3% de 1.246,162 empresas activas según el Instituto Nacional de Estadística y Censos (INEC) y la Cámara de Innovación y Tecnología Ecuatoriana (CITEC) en su boletín sobre la Situación del E-Commerce en Ecuador durante el 2023. Aquellas organizaciones pertenecerán al sector industrial, alimenticio, de seguridad y servicios que realicen el tipo de comercio B2C en la ciudad de Guayaquil, se indagará sobre las políticas internas, herramientas tecnológicas (como firewalls, encriptación, autenticación multifactorial), y los recursos humanos especializados en ciberseguridad. Los resultados serán representados en tablas y gráficos estadísticos. Además, se realizará un contraste con estudios previos sobre ciberseguridad en la región para verificar la consistencia de los resultados.

Finalmente, para lograr el último objetivo específico se aplicarán métodos estadísticos para examinar los datos obtenidos en la entrevista semiestructurada, a través de un análisis temático, facilitando la identificación de patrones comunes y diferencias en la ejecución de medidas de ciberseguridad y su efecto en la continuidad operativa. Este análisis conjunto permitirá determinar en qué medida las medidas de seguridad implementadas influyen en la capacidad de las organizaciones para mantener sus operaciones sin interrupciones significativas.

7. Resultados y discusión

Una vez que se han llevado a cabo las entrevistas a las 8 empresas que realicen el tipo de comercio B2C en la ciudad de Guayaquil, se procede a presentar un resumen de los comentarios recogidos en cada pregunta, como se evidencia a continuación:

Tabla 1
Análisis de las entrevistas

N.	Preguntas	Análisis de los comentarios
1	¿Qué tipo de amenazas cibernéticas ha enfrentado su organización en los últimos años relacionadas con el comercio electrónico?	De acuerdo con los entrevistados las principales amenazas que enfrentan con frecuencia son Ransomware, virus troyano, Phishing y otros que están relacionados con la extracción de datos confidenciales de las compañías.
2	¿Cuáles considera que son las amenazas cibernéticas más frecuentes o peligrosas para su empresa?	Las respuestas recopiladas coinciden en señalar que la amenaza común es el Phishing conocido como suplantación de identidad representa un alto riesgo debido al factor humano. Hemos detectado intentos recurrentes de engañar a colaboradores mediante correos fraudulentos que buscan obtener credenciales o acceso a información sensible.
3	¿Han experimentado incidentes de seguridad como phishing, ransomware, brechas de datos, o ataques DDoS? ¿Podría compartir un ejemplo si es posible?	Según los expertos, por medio de los correos empresariales envían enlaces maliciosos solicitando datos bancarios esto se ha intensificado en los últimos años.
4	¿Qué impacto han tenido estas amenazas en las operaciones diarias de su organización, especialmente en el canal de comercio electrónico?	En ocasiones presentan breves interrupciones en la atención al cliente ocasionando pérdidas en ventas, y la conexión de los servidores donde se almacena la información generando retrasos en las actividades operativas impactando significativamente las operaciones del negocio.
5	¿Cómo evalúan el nivel de riesgo cibernético actual al que están expuestos?	Mediante declaraciones señalan recibir a diario correos de múltiples direcciones con contenido publicitario o enlaces que suponen pérdida de tiempo y recursos; algunos tienen protección que permite que se envíen directamente a la carpeta de spam.

6	¿Qué medidas o estrategias de ciberseguridad ha implementado su organización para proteger sus plataformas de comercio electrónico?	Las respuestas obtenidas sobre las estrategias de ciberseguridad implementadas en su mayoría son los Software Antivirus y antimalware empresariales para proteger las plataformas de e-Commerce.
7	¿Qué tecnologías específicas utilizan para la protección de datos y sistemas (por ejemplo: firewalls, antivirus, autenticación multifactor, cifrado, etc.)?	Se utilizan la inteligencia artificial IA y el blockchain, antivirus protocolos HTTPS con certificados SSL, firewalls de aplicaciones web (WAF) y autenticación multifactorial (MFA), Gestores de contraseñas seguros que permiten el almacenamiento cifrado de datos y el fortalecimiento de políticas organizacionales.
8	¿Su empresa cuenta con un equipo especializado o departamento encargado exclusivamente de la ciberseguridad?	A partir de los resultados, se identificó que la gestión de la seguridad informática está a cargo del área de sistemas, lo cual ha sido funcional hasta cierto punto, ya que como tal no se cuenta con un departamento estructural para fortalecer los temas de ciberseguridad.
9	¿Qué tan frecuente es la actualización de sus políticas y protocolos de seguridad?	Resumiendo las respuestas, si cuentan con políticas internas de seguridad en las compañías pero no están siendo actualizadas, ni alineados completamente con los cambios tecnológicos y normativos más reciente.
10	¿Realizan capacitaciones internas sobre ciberseguridad para su personal?	En base a las contestaciones dadas, señalan que las capacitaciones sobre ciberseguridad son parcial e inexistentes, esto contribuye la vulnerabilidad de ataques cibernéticos, prolongando deficiencias de conocimiento en este ámbito.
11	¿Qué acciones específicas ha tomado su empresa para asegurar la continuidad operativa ante un ciberataque?	Se han implementado diversas acciones como Implementación de respaldos automáticos, contratación de software antivirus, monitoreo de transacciones en tiempo real, cambio continuo de contraseñas, PIN correspondiente a cada usuario.

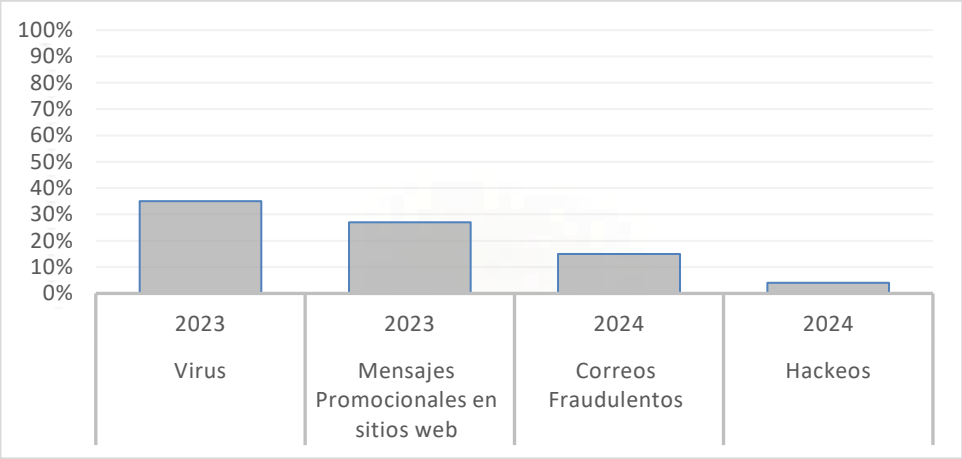
12	¿Cuentan con un plan de respuesta ante incidentes cibernéticos? ¿Ha sido puesto en práctica?	La mayoría de las organizaciones no disponen de un plan de respuesta. ante Ataques o alteraciones en sistemas informáticos, ni implementan normas legislativas nacionales e internacionales en base a estándares internacionales como ISO/IEC 27035 e ISO 22301.
13	¿Cómo evalúa la relación entre la inversión en ciberseguridad y la estabilidad de sus operaciones en línea?	Se logró identificar que, consideran que la inversión en ciberseguridad como protección de datos de las transacciones en línea de la compañía han reducido significativamente los sucesos de seguridad, esto es indispensable para la sostenibilidad del negocio.
14	¿Han medido o percibido mejoras en la continuidad operativa luego de implementar nuevas medidas de ciberseguridad?	Los entrevistados concluyeron que si han percibido mejoras significativas en la continuidad operativa, el rastreo y aviso de alertas sobre posibles virus cibernéticos ayudan a responder de forma más rápida y coordinada ante posibles amenazas.
15	Desde su experiencia, ¿qué tan crítica considera la ciberseguridad para garantizar el funcionamiento ininterrumpido del comercio electrónico en su organización?	Con respecto a las experiencias compartidas, la ciberseguridad representa un aspecto fundamental para asegurar la continuidad de nuestras operaciones en comercio electrónico, han optado medidas preventivas como el uso de plataformas seguras, Usuarios y contraseñas seguras, respaldo en disco duro, que protejan los datos e información de los clientes.

Fuente: Elaboración Propia

Mediante el análisis realizado, se identificarán las amenazas cibernéticas más frecuentes que afectan a las organizaciones ecuatorianas que operan en entorno al comercio electrónico. Estos ataques incluyen delitos de phishing, ransomware, malware, y denegación de servicios (DDoS) los cuales representan riesgos significativos para seguridad de las transacciones y la integridad de los datos relevantes para las compañías.

A continuación, se presenta el siguiente gráfico, datos reales obtenidos mediante el recurso de entrevista semiestructura sobre los recurrentes fallas o vulneraciones en entornos digitales a los que están expuestos y la adopción de tecnologías emergentes.

Gráfico 1. Amenazas Cibernéticas Reportadas por Organizaciones en Ecuador



Fuente: Elaboración Propia

Según los hallazgos de este estudio, los virus representan el 35% relacionado a 4 empresas dedicadas al comercio electrónico, seguido de los mensajes promocionales a través de sitios web en un 27% correspondiente a 2 empresas entrevistadas, otros ataques más comunes son los correos fraudulentos y hackeos representando un 15% y 10% representan a 2 empresas que han detectado estos tipos de acontecimientos de ciberseguridad comprometiendo sus sistemas.

A partir de las respuestas proporcionadas por los entrevistados, se reconocen distintos tipos de ataque; siendo los virus o malware lo que a menudo se difunden a través de correos electrónicos, consolidando una de las estrategias más empleadas por los delincuentes cibernéticos por su gran complejidad de rastreo de origen y la atribución de los responsables. En un entorno precipitado del crecimiento del comercio electrónico, es esencial prevenir y controlar delitos para optimizar la prevención, identificación y reacción frente a amenazas a la seguridad digital.

Bajo este marco, "De acuerdo con el más reciente informe de ciberseguridad de Check Point, Ecuador se halla en una situación alarmante en cuanto a amenazas cibernéticas para el 2024. Con una subida del 4,9 % en comparación con el año previo, el país percibe un riesgo del 51,9 %, situándose como el tercer país más amenazado en América Latina, tras Perú y Colombia" (El Universo, 2024 párr. 1). Esta información prevalece cómo Ecuador se ve forzado a implementar la integración de medidas tecnológicas avanzadas y políticas organizacionales para potenciar de manera complementaria las capacidades de responder y solucionar estas coacciones frente a un entorno vulnerable cibernético en constante evolución.

En el contexto ecuatoriano, los delitos cibernéticos han mostrado un desarrollo sostenido, lo cual ha sido documentado por diversas entidades nacionales e internacionales. La siguiente tabla ostenta una breve sinopsis de las principales amenazas identificadas por Instituciones Oficiales las cuales son: Centro de Respuesta a Incidentes de Seguridad EcuCERT(2024), Cámara Ecuatoriana de Comercio Electrónico CECE (2024), el Ministerio de Telecomunicaciones y de la Sociedad de la Información MINTEL (2023), la Agencia de Regulación y Control de las Telecomunicaciones Arcotel (2023) y la empresa de ciberseguridad Check Point (2024).

Tabla 2. Principales Delitos Cibernéticos En Ecuador Basada En Fuentes Oficiales

Amenaza Cibernética	Observaciones	Fuente Principal
PHISHING	De alta recurrencia en plataformas de comercio electrónico	EcuCERT2024
RANSOMWARE	Impacta directamente en funciones clave de la organización.	MINTEL 2023
ATAQUES DDOS	Interrupción servicios web.	Check Point 2024
INGENIERÍA SOCIAL	Mayor incidencia en perfiles que carecen de capacitación especializada.	CECE 2024
MALWARE	Ejecutado a través de vínculos maliciosos.	Arcotel 2023
SUPLANTACIÓN DE IDENTIDAD	Estafas recurrentes en plataformas digitales (sitios web)	CECE 2018
FUGAS DE INFORMACIÓN	Brechas de seguridad originadas por una gestión incorrecta de la información	MINTEL 2023
ACCESO NO AUTORIZADO	Utilizan fallos en los mecanismos de protección para sus fines.	Check Point 2024

Fuente: Elaboración propia con base en CECE (2024), MINTEL (2023), Arcotel (2023), y Check Point (2024).

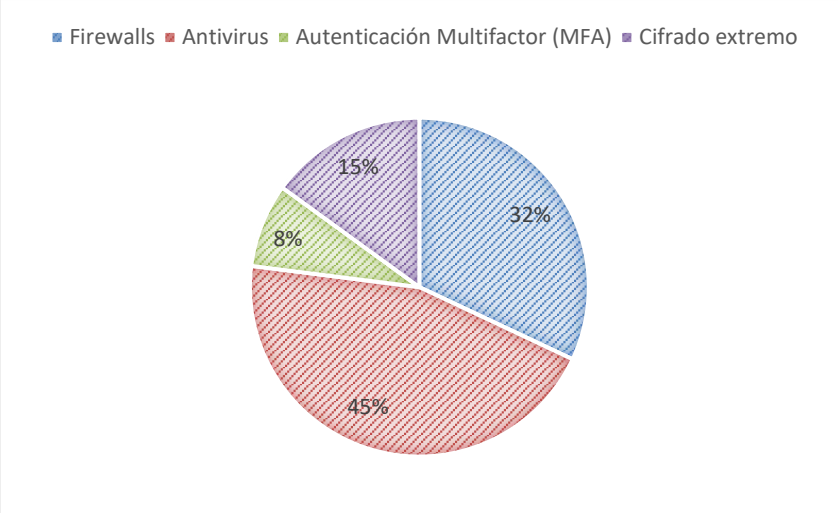
Según lo evidenciado en el análisis, los ataques que encabezan la lista de los más frecuentes son: Según García García (2018), el phishing es un tipo de fraude online que busca robar al usuario, entre otros, información, contraseñas o números de cuentas bancarias para obtener un beneficio económico ilegal mediante el engaño del mismo. Asimismo, Moreno, J., Rodríguez, C., & Leguías, I. (2019) definen al ransomware como una nueva amenaza que azota a la humanidad, enfocándose en

los sistemas operativos de Windows para escritorio. Pero también señalan que los teléfonos y ordenadores sufren robo, pérdida de datos y secuestro de información, amenazando la seguridad personal.

En síntesis, estos casos suelen involucrar la suplantación de identidad, afectando a los sectores económico, financiero, comercial, retail, salud y plataformas bancarias locales, comprometiendo información sensible de las organizaciones ecuatorianas que operan en el comercio electrónico en Guayaquil, muchas de las cuales carecen de una infraestructura firme en ciberseguridad.

Por otra parte, en el gráfico siguiente se muestran los resultados de la evaluación de las estrategias y tecnologías de ciberseguridad implementadas por las organizaciones ecuatorianas en el comercio electrónico, describiendo las principales herramientas tecnológicas y políticas adoptadas por las empresas, tanto en su enfoque preventivo como en la capacidad de mitigación de riesgos, esto será esencial para analizar las oportunas respuestas ante contingencias digitales

Gráfico 2. Estrategias y tecnologías de ciberseguridad



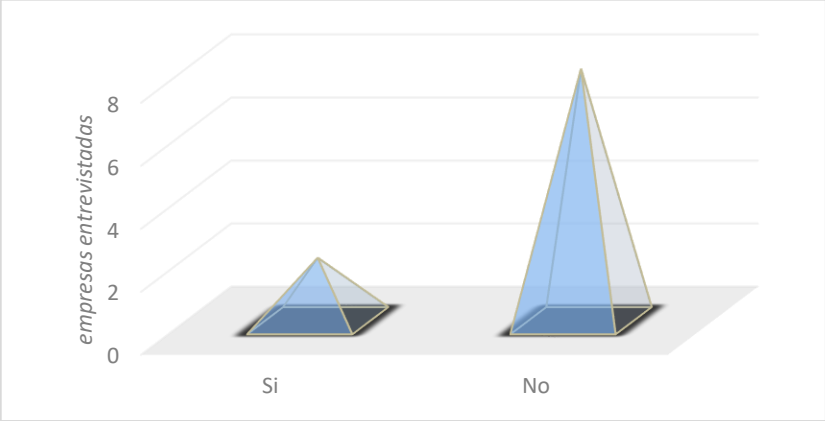
Fuente: Elaboración Propia.

Se identificaron que el 45 % equivalente a (3) organizaciones priorizan la adquisición de software antivirus enfocado en detectar y eliminar malware, especialmente después de que este pone en riesgo el sistema. Seguidamente, se destaca en un 32% (2) hace uso de firewalls, que funcionan como barreras de seguridad para regular el tráfico de red y prevenir accesos no autorizados. El 15%(2) manejan el cifrado extremo como método de seguridad ya que asegura que únicamente el emisor y el receptor tengan acceso a los mensajes. Y por último el 8% (1) utiliza la Autenticación multifactorial (MFA) sea contraseñas o PIN que supervisen o examinan el tráfico de red con el fin de identificar actividades sospechosas o potencialmente dañinas.

Los indicares analizados evidencian un compromiso a través la adopción de tecnologías para salvaguardar datos, como sistemas de detección de intrusos (IDS), políticas de respaldo periódico. Asimismo, la protección y resguardo de datos en la nube es esencial, utilizando tecnologías avanzadas como el cifrado de información y accesos controlados basados en (IA) son mecanismos que refuerzan la protección al exigir verificaciones adicionales permiten establecer una base firme para la creación de estrategias preventivas que fortalezcan el progreso tecnológico de las compañías.

De manera complementaria, dentro del análisis de las estrategias de ciberseguridad, el siguiente gráfico muestra la capacitación continua del personal, considerada una de las acciones fundamentales y más eficaces para reducir los riesgos asociados al del factor humano.

Gráfico 3. Capacitación en Ciberseguridad Impartidas al Personal



Fuente: Elaboración Propia.

Los resultados obtenidos indican un número significativo de organizaciones en Ecuador que no implementan programas de capacitación, políticas internas, ni actividades de concienciación en ciberseguridad para su personal. Esto fomenta una escasa cultura organizacional sobre la adopción de tecnologías emergentes y medidas organizacionales, frente a ello se encuentran el fortalecimiento de capacidades técnicas, la colaboración interinstitucional y la adopción de estándares internacionales como ISO/IEC 27001 son pasos clave para mejorar la seguridad del ciberespacio en el país.

De acuerdo con este tema, la Cámara Ecuatoriana de Comercio Electrónico (CECE) juega un rol clave en mejorar la ciberseguridad y el comercio electrónico en el país. A través de iniciativas como el e-Commerce Day Ecuador, coorganizado con el e-Commerce Institute, la CECE promueve la capacitación y certificación en prácticas de seguridad para el comercio en línea, con el objetivo de reforzar la confianza del

consumidor y proteger las transacciones digitales. De igual manera, colabora activamente en el desarrollo de políticas públicas sobre comercio electrónico y ciberseguridad, junto al Ministerio de Telecomunicaciones y la Sociedad de la Información (MINTEL) (CECE, 2025).

También se llevó a cabo un contraste con estudios previos sobre ciberseguridad en la región para comprobar la consistencia de los resultados. Asimismo, se incluye información actualizada sobre los índices de ciberseguridad con el fin de complementar el enfoque principal.

En esta línea (Aguilar, 2021) subraya que América Latina enfrenta retos significativos en la creación de políticas de ciberseguridad y en mejorar las capacidades para tratar riesgos y amenazas cibernéticas, particularmente en áreas que afectan la seguridad nacional y la política exterior (párr. 01).

Este estudio presenta información proporcionada por organismos internacionales que evalúan y promueven políticas de ciberseguridad, midiendo el nivel de compromiso e importancia que los Estados otorgan dentro de sus políticas nacionales. Entre estos se encuentran el Índice Global de Ciberseguridad (GCI, por sus siglas en inglés), elaborado por la Unión Internacional de Telecomunicaciones (UIT, 2022); la Organización de Estados Americanos (OEA, 2023); el Banco Interamericano de Desarrollo (BID, 2022); y la Comisión Económica para América Latina y el Caribe (CEPAL, 2023).

En relación al informe preparado por la OEA y el Banco Interamericano BID titulado Ciberseguridad: *¿Estamos preparados en América Latina y el Caribe?,* subraya la importancia de desarrollar estrategias de ciberseguridad en países de América Latina y el Caribe (ALC). Colombia, Jamaica, Panamá y Trinidad y Tobago ya cuentan una estrategia en marcha; asimismo se están desarrollando en países como Costa Rica, Dominica, Perú, Paraguay y Surinam. (OEA & BID, 2016).

Por otro lado, el informe *Ciberseguridad 2020: riesgos, avances y el camino a seguir en América Latina y el Caribe* indica que solo 17 de los 32 países analizados en la región cuentan con estrategias nacionales de ciberseguridad aprobadas (OEA & BID, 2020). Estos antecedentes investigativos buscan medir y comparar el desarrollo de políticas públicas, capacidades técnicas e institucionales, y niveles de cooperación regional en los países latinoamericanos, teniendo en cuenta las características específicas y las diferencias propias de cada país.

No obstante, a pesar de ciertos avances estructurales, el horizonte actual sigue siendo desafiante. El portal TechTegia, referenciado en el informe del Banco Interamericano de Desarrollo exterioriza que la región enfrenta “más de 1 600

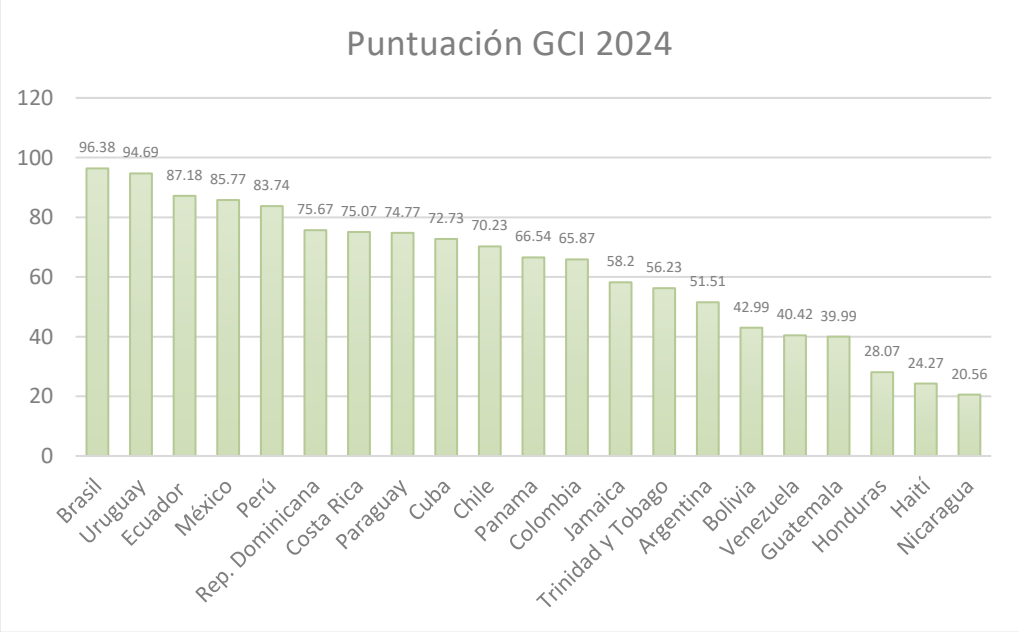
ciberataques por segundo" entre 2022 y 2023 (BID, 2024).

La digitalización y la adopción de tecnología es desigual a nivel regional dependen de varios factores, como la disponibilidad de Internet y de los servicios digitales (gobierno electrónico, comercio electrónico). Brasil y México encabezan el ranking regional de ciberataques, acumulando 23 000 y 14 000 millones de detecciones respectivamente en la primera mitad de 2023 (Arrieta, 2024).

De acuerdo con el Índice Global de Ciberseguridad, Brasil y Uruguay destacan con los niveles más altos de madurez en ciberseguridad (Unión Internacional de Telecomunicaciones [UIT], 2024). En comparación con otras naciones que aún presentan rezagos en este ámbito, Ecuador y Panamá en 2024, han logrado avances significativos en el promedio global y posicionándose como referentes emergentes en la región.

Para profundizar el análisis regional, en el siguiente gráfico presenta los datos del Índice Global de Ciberseguridad (GCI) en América Latina, fundamentado en la valoración de cinco pilares fundamentales: legal, técnico, organizacional, capacitación y colaboración para crear un entorno seguro en el progreso de la tecnología de la información.

Gráfico 4. Índice Global de Ciberseguridad (GCI) Latinoamérica 2024



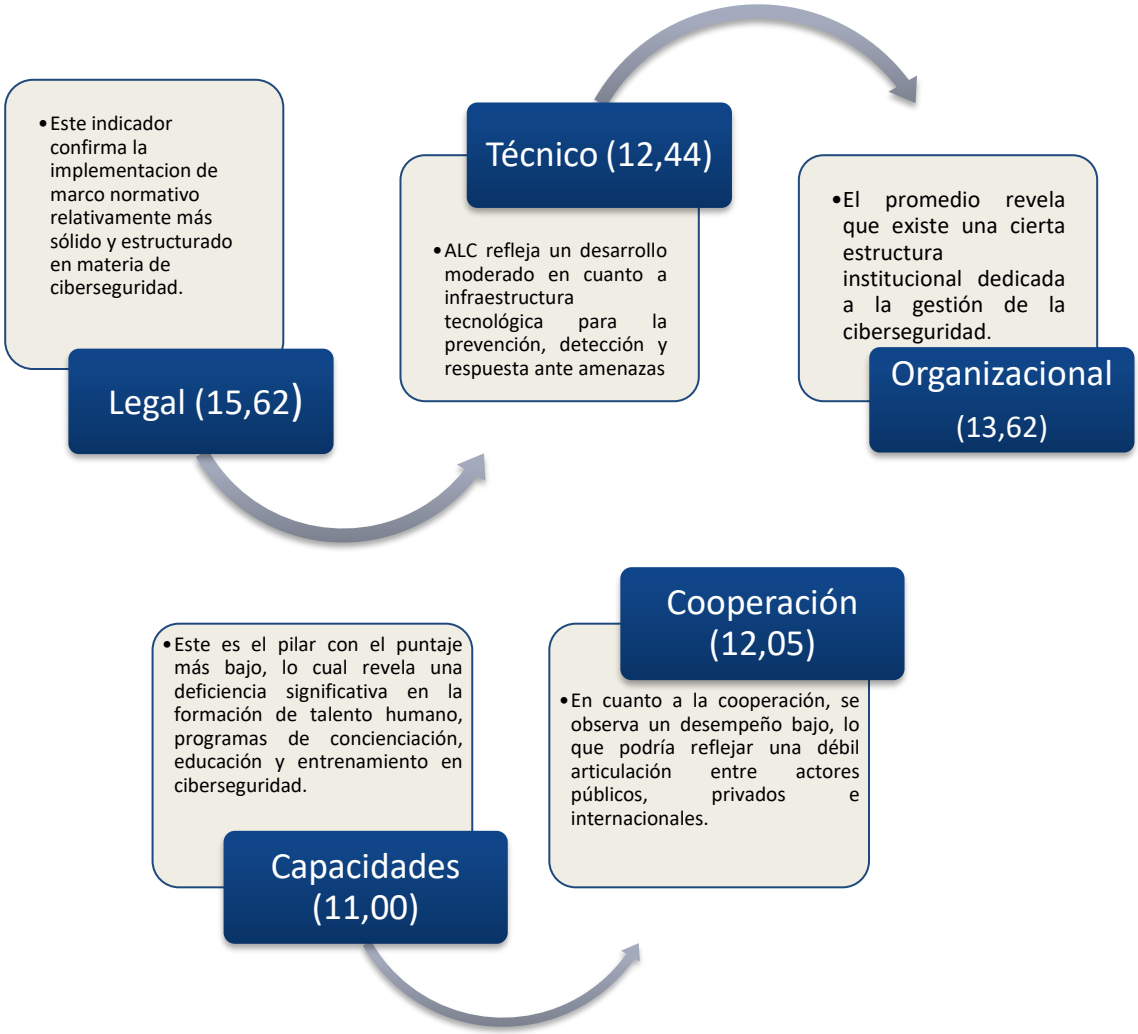
Fuente: Elaboración propia basada en datos del Índice Global de Ciberseguridad (UIT, 2024).

Los datos ilustrados en esta publicación muestran una marcada heterogeneidad en América Latina, los países con mayor desempeño en el avance de la ciberseguridad

son: Brasil, Uruguay, México, Ecuador, Perú. Mientras que una minoría enfrenta retos significativos para fortalecer su infraestructura tecnológica, gobernanza organizacional y desarrollo de talento humano. De acuerdo con Zambrano Rendón et al. (2024), es necesario llevar a cabo un esfuerzo coordinado y continuo que abarque el refuerzo de las políticas de ciberseguridad, la promoción de la formación y el aumento de la conciencia, así como el impulso de la cooperación regional para combatir esta amenaza que sigue cambiando, asegurando así la protección de los activos digitales.

Se realizó el cálculo del promedio de los valores obtenidos tras el análisis cualitativo y cuantitativo de la información recopilada en los los cinco pilares evaluados, como medida de tendencia central la cual permitirá identificar tendencias generales y comparativas entre los distintos ámbitos que maneja América latina en la actualidad.

Gráfico 5. Promedio Pilares de Índice Global de Ciberseguridad (GCI) Latinoamérica 2024



Fuente: Elaboración Propia.

Finalmente, mostraremos la relación entre la eficacia de las acciones de ciberseguridad y la habilidad de las entidades ecuatorianas en el comercio electrónico, se evaluará la eficiencia de la continuidad operativa ante los riesgos cibernéticos que se encuentran expuestos. Inicialmente a través del siguiente análisis sistemático se muestran los patrones comunes y diferenciales indicados por los entrevistados:

Tabla 3. Ciberseguridad y continuidad operativa en las organizaciones de Ecuador

N.	Empresa	Proteccion Tecnica Infraestructura)	Cumplimiento Legal (LOPD)	Gestion Organizacional	Continuidad Operativa del Negocio (Nivel de Impacto)
1	Traimex S.A.	✓ Implementación de backups diarios y firewall en nube.	✓Cumplen con normativas legales	✓Cultura sólida, protocolos claros de seguridad	3
2	Hiberus S.A.	✓ Enlace alterno de internet y sistema de alertas.	◆Cumplimiento parcial	○ No existen politicas, ni capacitación	2
3	Veles & Asesores	◆ Planes de contingencia unicamente en caso de ataque digital.	◆Cumplimiento parcial	○ No existen politicas, ni capacitación	1
4	Signature S.A.	✓Contratación de sistema de alertas.	✓Cumplen normativas legales	✓Cultura sólida, protocolos claros de seguridad	3
5	Tipti S.A.	✓ Usan HTTPS, firewalls Alojamiento en servidores seguros.	◆Cumplimiento parcial	◆Se basan en politicas internas.	2
6	Sypsocia S. A	✓Backups automáticos diarios y replicación en la nube	◆Cumplimiento parcial	○ No realizan capacitaciones, solo simulacros anuales.	2
7	Carsicurity Cia Ltda	✓ Revisión semanales y monitoreo en tiempo real.	✓Cumplen con normativas legales	✓Capacitaciones recurrentes de seguridad	3

8	Ceroriesgo S.A.	✓ Inversión en ciberseguridad y simulacros de ataque	◆ Cumplimiento parcial	○ No realizan capacitaciones	1

Fuente: Elaboración propia.

Los datos fueron codificados simbólicamente:

✓ = representado en valor alto 3.

◆ = representado en valor mediano 2.

○ = representado en valor bajo 1.

Posteriormente para la correlación directa entre la continuidad operativa y los niveles medidos, se aplicó un análisis estadístico que incluyó el cálculo del Alfa de Cronbach y un análisis de regresión lineal para validar la consistencia interna de las respuestas obtenidas:

- **Variable Independiente:** Protección técnica, legal, gestión organizacional.
- **Variable Dependiente**: Continuidad operativa del negocio.

Tabla 4. Resultados de Indicadores Estadísticos

Ítem	**Valor Estadístico**	**Interpretación**
Alfa de Cronbach	0.83	Alta consistencia interna
Coeficiente de Regresión	0.70	Fuerte correlación positiva
Valor-p (regresión)	0.02	Estadísticamente Significativo

Fuente: Elaboración propia con base en resultados de SPSS

El resultado obtenido del análisis del Alfa de Cronbach fue de 0.83, lo cual indica una buena consistencia interna de los ítems que componen las 3 dimensiones: técnica, legal y organizacional “medidas de ciberseguridad" frente al grado de preparación de las organizaciones que amenacen la continuidad operativa en el comercio electrónico. De acuerdo con el criterio de George y Mallery (2003), un valor de $\alpha \geq 0.80$ se considera aceptable, lo cual respalda estadísticamente la validez y confiabilidad del instrumento aplicado.

En relación al análisis de regresión lineal con un resultado de coeficiente de regresión de b = 0.70 y valor-p de 0.002, indican que este efecto es estadísticamente

significativo evidenciando que las medidas de seguridad ejercen un efecto positivo y significativo sobre la continuidad operativa de las organizaciones.

En síntesis, se observa que la mayoría de las organizaciones analizadas en su visión técnica disponen de planes de contingencia para mitigar el impacto de ataques cibernéticos, las mismas implementan mecanismos preventivos que incluyen estrategias de respaldo de datos, contratación de software cibernéticos, ejecución periódica de simulacros, así como la adopción de sistemas avanzados de detección.

En el ámbito legal, la ciberseguridad en Ecuador adopta marcos normativos nacionales e internacionales, entre los que destacan la Ley Orgánica de Protección de Datos Personales y las recomendaciones del Instituto Ecuatoriano de Normalización (INEN) es alinearse a estándares internacionales ISO 22301 (Gestión de la Continuidad del Negocio) e ISO/IEC 27001 (Seguridad de la Información), estas normativas no se cumplen de forma integral en la práctica, lo que muestra la necesidad de mejorar su aplicación. De igual manera, se identifica una debilidad estructural a nivel organizacional, ya que no capacitan de forma continua al personal ni actualizan sus políticas internas, lo cual limita la efectividad del factor humano como primera línea de defensa frente a compromisos de seguridad digital.

Los hallazgos de esta investigación destacan que organizaciones ecuatorianas dedicadas al comercio electrónico enfrentan una diversidad de amenazas cibernéticas, entre las que reinciden el *phishing*, los virus troyanos y el *ransomware*. A pesar del conocimiento general sobre los riesgos digitales, la mayoría de las organizaciones entrevistadas carecen de un departamento especializado en ciberseguridad, delegando esta responsabilidad al área de sistemas. En este sentido, Boné-Andrade (2023), advierte la ciberseguridad en entornos empresariales actuales enfrenta desafíos cada vez más sofisticados, impulsados en gran medida por el avance de tecnologías como la Inteligencia Artificial y el machine learning. Respecto a las estrategias implementadas, se evidencio el uso de software de protección firewalls, copias de seguridad y mecanismos de autenticación, indispensable para corregir las deficiencias estructurales que afectan la sostenibilidad operativa de los negocios. En cuanto a la relación entre la inversión en ciberseguridad y la estabilidad operativa, las respuestas coinciden en reconocer que la aplicación de medidas de protección ha facilitado avances notables en la respuesta a incidentes y en la estabilidad de las transacciones. Este punto refuerza lo planteado por Saphirtek (2024), al destacar que el fortalecimiento de la seguridad informática es clave para reducir el impacto económico y operativo de los ataques. Finalmente, la ausencia capacitación continua al talento humano respaldado por políticas integrales y normativas legales limita la capacidad de defenderse a los ciberataques. Como lo destaca Gupta (2024), “la importancia del cumplimiento legal y regulatorio [...] subraya la necesidad de un enfoque proactivo y

multifacético” en la ciberseguridad para entornos de comercio electrónico. Por lo que afecta directamente en la estabilidad del mismo generando una ciberseguridad poco proactiva.

8. Conclusión

Para culminar el estudio de los resultados logrados mediante entrevistas a representantes de organizaciones ecuatorianas en función a los objetivos planteados, se concluye que las amenazas cibernéticas más frecuentes en el entorno digital son el phishing y el ransomware y los ataques mediante virus troyanos los más habituales, especialmente aquellas relacionadas con la suplantación de identidad, se complican por el factor humano, es decir, por la ausencia de preparación y concienciación del personal en cuanto a prácticas seguras de navegación y uso de plataformas digitales.

Se constató las estrategias y tecnologías de protección digital aplicadas que las empresas han incorporado para salvaguardar sus operaciones, entre las que destacan los antivirus corporativos, firewalls, autenticación multifactorial, certificados SSL y sistemas de monitoreo. Ecuador ha mostrado avances importantes en materia de ciberseguridad, no obstante, se mantienen limitaciones en la aplicación adecuada de políticas, la formación constante del personal y la adherencia a normativas.

Se identificó una conexión directa entre la eficacia de las acciones de ciberseguridad y la habilidad de las empresas para sostener la continuidad de sus operaciones. Las organizaciones que han invertido en mecanismos de protección robustos y prácticas preventivas han logrado minimizar interrupciones que permiten responder con mayor agilidad ante incidentes.

Se han alcanzado avances significativos en la ejecución de estrategias de ciberseguridad, aún es fundamental mejorar la cultura organizativa en cuanto a la seguridad digital, establecer políticas actualizadas de manera institucional, y adaptar las prácticas a estándares internacionales que aseguren la continuidad de las actividades en un entorno más expuesto a amenazas tecnológicas.

9. Referencias Bibliográficas.

Agencia de Regulación y Control de las Telecomunicaciones. (2023). Estadísticas de incidentes informáticos en el sector TIC ecuatoriano. https://www.arcotel.gob.ec/

Aguilar Antonio, J. M. (2021). Retos y oportunidades en materia de ciberseguridad de América Latina frente al contexto global de ciberamenazas a la seguridad nacional y política exterior. Estudios Internacionales, 53(198), 169–197. https://doi.org/10.5354/0719-3769.2021.57067

Álvarez-Teleña, S., & Díez-Fernández, M. (2024, 14 de octubre). Ciberseguridad moderna: Nueva era, nuevas estrategias. SSRN. https://ssrn.com/abstract=4991580

Asamblea Nacional del Ecuador. (2021). Ley Orgánica de Protección de Datos Personales [Registro Oficial Suplemento No. 459, 26 de mayo de 2021]

Arrieta, F. (2024, 22 de julio). Brasil y México lideran ranking de ciberataques. Prensario. Recuperado de https://www.prensario.net/Brasil-y-Mexico-lideran-ranking-de-ciberataques-46224.note.aspx

Banco Interamericano de Desarrollo. (2024). Informe sobre ciberataques en América Latina. https://www.iadb.org

Banco Interamericano de Desarrollo, & Organización de los Estados Americanos. (2016). Ciberseguridad: ¿Estamos preparados en América Latina y el Caribe? https://doi.org/10.18235/0006517

Barzola, L., Jara, J., & Avilés, P. (2019). Importancia del marketing digital en el comercio electrónico. E-IDEA Journal of Business Sciences, 1(3), 24–33. https://revista.estudioidea.org/ojs/index.php/eidea/article/view/14

Becerril, A. (2019). La ciberseguridad en los tratados de libre comercio. Revista Chilena de Derecho y Tecnología, 8(2), 111–137

Becerril Gil, A. A., & Ortigoza Limón, S. (2018). Habilitadores tecnológicos y realidades del Derecho Informático Empresarial. Revista Ius, 12(41), 11–41

Bhargava, R. (2020). Small business cybersecurity: The cost of breaches and recovery strategies. Journal of Business Continuity and Risk Management, 12(3), 215–230. https://doi.org/10.1234/jbcrm.2020.00234

Boné-Andrade, M. F. (2023). Evaluación de la evolución de la ciberseguridad en sistemas empresariales modernos. Multidisciplinary Collaborative Journal, 1(2), 25–38. https://doi.org/10.70881/mcj/v1/n2/14

Cámara Ecuatoriana de Comercio Electrónico. (2022). Resultados de la V medición del estudio de comercio electrónico en Ecuador.

https://online.uees.edu.ec/investigacion/presentacion-de-resultados-del-estudio-de-transacciones-no-presenciales-en-ecuador

Cámara Ecuatoriana de Comercio Electrónico. (2023). Estudio Escomerse 2023 - VI Medición de comercio electrónico en Ecuador. https://online.uees.edu.ec/investigacion/estudio-de-comercio-2023

Cámara Ecuatoriana de Comercio Electrónico (CECE). (2024). Informe anual de comercio electrónico en Ecuador 2023. https://cece.ec

Cámara Ecuatoriana de Comercio Electrónico. (2025, junio). El eCommerce Day llega a Ecuador con edición 100 % online. https://cece.ec/el-ecommerce-day-llega-a-ecuador-con-edicion-100-online/

Calle García, A. J., Conforme Merchán, Y. M., Magallanes Bueno, E. L., & Guaranda Bravo, J. Y. (2024). Importancia de la ciberseguridad en la investigación de mercados digital. Ciencia y Desarrollo, 27(2), 257–263. https://dialnet.unirioja.es/servlet/articulo?codigo=9604359

Castells, M. (2001). Internet y la sociedad red [PDF]. https://trabajosocialunam.files.wordpress.com/2014/08/manuel-castells-internet-y-la-sociedad-de-la-informacic3b3n.pdf

Centro de Respuesta a Incidentes Informáticos del Ecuador (EcuCERT). (2024, 22 de julio). AL-2024-15: Incidente global en sistemas Windows 10 y 11 tras actualización de CrowdStrike Falcon Sensor. https://www.ecucert.gob.ec/wp-content/uploads/2024/07/AL-2024-15-Crowdstrike.pdf

Check Point Software Technologies. (2024). Cyber security report: Latin America threat landscape. https://www.checkpoint.com

Chinchilla Morales, J. (2021, marzo). La ciberseguridad [Informe técnico, Universidad Técnica Nacional – Sede Regional Chorotega]. Repositorio Institucional USAM. https://repositorio.usam.ac.cr/xmlui/handle/11506/2392

Chevalier, S. (2024, enero 31). El comercio electrónico sigue creciendo en América Latina. Statista. https://es.statista.com/grafico/22835/boom-del-ecommerce-en-latinoamerica/

Diego, I. M. D., & Fernández Isabel, A. (2020). Ciencia de datos para la ciberseguridad (1ª ed.). RA-MA Editorial. https://bibliotecas.ups.edu.ec:3488/es/ereader/bibliotecaups/222714?page=18

El Universo. (2024, abril 16). Ciberseguridad y protección de datos: Un desafío estratégico para las empresas en Ecuador. https://itahora.com/amp/2025/04/16/ciberseguridad-y-proteccion-de-datos-un-desafio-estrategico-para-las-empresas-en-ecuador/

EMarketer. (2024). Latin America retail eCommerce sales 2024–2028. Insider Itelligence. https://www.insiderintelligence.com/content/latin-america-retail-ecommerce-sales-2024

Fezzey, T., Batchelor, J. H., Burch, G. F., & Reid, R. (2023). Cybersecurity continuity risks: Lessons learned from the COVID-19 pandemic. Journal of Cybersecurity Education, Research and Practice. Recuperado de https://eric.ed.gov/?id=EJ1387214

García García, D. E. (2018). El phishing como delito de estafa informática. Comentario a la SAP de Valencia 37/2017 de 25 de enero (rec. 1402/2016). Revista Boliviana de Derecho, (25), 650–659. https://dialnet.unirioja.es/servlet/articulo?codigo=6263417

George, D., & Mallery, P. (2003). SPSS for Windows step by step: A simple guide and reference (4th ed.). Allyn & Bacon

González, I. Á., & Sanz, R. M. (2020). Comercio electrónico y redes de producción global. Ekonomiaz: Revista vasca de economía, (98), 278–295

Grillo, S. F. S. (2021). El comercio electrónico y su incidencia en el desarrollo empresarial. Dominio de las Ciencias, 7(2), 824–844. https://go.gale.com/ps/i.do?id=GALE%7CA693364770&sid=googleScholar&v=2.1&it=r&linkaccess=abs

Gupta, R. (2024). Cybersecurity threats in e-commerce: Trends and mitigation strategies. Journal of Advanced Management Studies, 1(3), 1–10. https://doi.org/10.36676/jams.v1.i3.13

Herrero Jiménez, M. (2021). La protección del consumidor en el comercio electrónico transfronterizo. Editorial Reus

Hashemi-Pour, C., & Lutkevich, B. (2023, 13 de diciembre). What is e-commerce? SearchCIO. TechTarget. Recuperado de https://www.techtarget.com/searchcio/definition/e-commerce?utm_source

Instituto Nacional de Estadística y Censos. (2024, abril). Registro Estadístico de Empresas 2023. https://www.ecuadorencifras.gob.ec/documentos/webinec/Estadisticas_Economicas/Registro_Empresas_Establecimientos/2023/Semestre_I/Boletin_REEM_2023.pdf

International Organization for Standardization, & International Electrotechnical Commission. (2022). ISO/IEC 27001:2022 — Information security, cybersecurity and privacy protection — Information security management systems — Requirements. https://www.iso.org/standard/82875.html

International Telecommunication Union. (2024). Global Cybersecurity Index (GCI) 2024. https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

Lin, H. (2024, abril 8). E-commerce statistics and trends for 2024 and beyond. Shopify. https://www.shopify.com/blog/ecommerce-statistics

Medina, C., Fernández, J., Borrero, P., & Alvear, J. L. (2019). Estrategias financieras en PYMES emergentes. Revista de Gestión Empresarial, X(Y), pp–pp. https://revista.gnerando.org/revista/index.php/RCMG/article/download/451/445/1895

Meyer, B. (2020). Cyber threats in the digital age: A review of e-commerce vulnerabilities. Journal of Information Security and Privacy, 16(3), 45–67

Ministerio de Telecomunicaciones y de la Sociedad de la Información. (2022). *Estrategia Nacional de Ciberseguridad del Ecuador 2022–2025*

Moreno, F., & Velázquez, J. (2019). Ciberseguridad y la protección de datos en el comercio electrónico en Latinoamérica. Seguridad Digital en Iberoamérica, 12(3), 120–135

Moreno, J., Rodríguez, C., & Leguías, I. (2019). Revisión sobre propagación de ransomware en sistemas operativos Windows. Revista de I+D Tecnológico, 2019(1), 45–57. Universidad Tecnológica de Panamá. https://portal.amelica.org/ameli/journal/339/3391488005/3391488005.pdf

Morales-Sáenz, F. I., Medina-Quintero, J. M., & Reyna-Castillo, M. (2024). Beyond data protection: Exploring the convergence between cybersecurity and sustainable development in business. Sustainability, 16(14), 5884. https://doi.org/10.3390/su16145884

Orus, A. (2024, 24 de mayo). Facturación mundial del comercio electrónico 2014-2027. Statista. https://es.statista.com/estadisticas/1242096/facturacion-delcomercio-electronico-mundial/

Paz, S. (2021). Economía digital: El futuro ya llegó (1.ª ed.). Universidad Nacional de Quilmes, Unidad de Publicaciones del Departamento de Economía y Administración. https://ridaa.unq.edu.ar/handle/20.500.11807/2990

Ramos-Secaira, R. (2023). La ciberseguridad como estrategia tecnológica en las organizaciones. Revista Científica CZ Ambato, 3(2), 51–66. https://revistaczambos.utelvtsd.edu.ec/index.php/home/article/view/47/97

Robayo-Botiva, D. M. (2020). El comercio electrónico: concepto, características e importancia en las organizaciones (Generación de contenidos impresos N.° 20). Ediciones Universidad Cooperativa de Colombia. https://doi.org/10.16925/gclc.13

San Román, A. P. (2019). Una visión de conjunto de la Globalización 4.0. Economistas (núm. 165), 9–13. Colegio de Economistas de Madrid. https://www.cemad.es/wp-content/uploads/2019/10/Vision-globalizacion-4-0.pdf

Saphirtek. (2024, octubre 22). Ciberataques en Ecuador: alarmante aumento en 2024. https://www.saphirtek.com/post/ciberataques-en-ecuador-alarmante-aumento-en-2024

Techtegia. (2024, junio 25). Informe integral sobre Ciberseguridad en América Latina para iniciar la gestión en 2024. https://techtegia.com/2024/06/informe-integral-sobre-ciberseguridad-en-america-latina-para-iniciar-la-gestion-en-2024/

UNCTAD. (2019). Informe sobre la economía digital 2019: Panorama general (págs. 5-10). Conferencia de las Naciones Unidas sobre Comercio y Desarrollo. https://unctad.org/system/files/official-document/der2019_es.pdf

Valarezo, V. (2020). Importancia de la ciberseguridad en el comercio electrónico. Universidad Técnica de Ambato. https://repositorio.uta.edu.ec/handle/123456789/31790

Zambrano Rendón, A. D., Meza Talledo, Y. K., Villavicencio Mendoza, C. M., & Rodríguez Zambrano, A. R. (2024). Ciberataques en América Latina: desafíos de la era digital. Compromiso Social. Revista de la UNAN-Managua, Extensión Universitaria, 1(13), 89–103. https://doi.org/10.5377/recoso.v1i13.19295