Sinergia Académica ISSN: 2765-8252

Volumen: 7
Nro. 4
Año: 2024

Recepción: 08-07-2024 / Revisión: 13-09-2024 / Aprobación: 29-09-2024 / Publicación: 27-10-2024

Impacto de los delitos informáticos en la economía empresarial del Ecuador

Impact of computer crimes on the business economy of Ecuador

Magali Paulina Coello Peralta[1] (mcoellop@unemi.edu.ec) (https://orcid.org/0009-0005-7373-1781)

Marcelo Xavier Godoy Heredia[2] (mgodoyh@unemi.edu.ec) (https://orcid.org/0009-0001-2985-5841)

Christian Marcelo Taco Barragán[3] (ctacob@unemi.edu.ec) (https://orcid.org/0009-0005-4260-7059)

Diego Marcelo Villamarin Irazábal[4] (dvillamarini@unemi.edu.ec) (https://orcid.org/0009-0001-1462-1217)

Enrique Colon Ferruzola Gómez[5] (eferruzolag@unemi.edu.ec) (https://orcid.org/0000-0002-6842-9634)

Holguer Estuardo Romero Urréa[6] (hromerou@unemi.edu.ec) (https://orcid.org/0000-0002-0877-0339)

Resumen

El estudio abordó el problema de cómo los delitos informáticos afectaron la economía empresarial en Ecuador, destacando la falta de medidas adecuadas de protección a pesar de los avances tecnológicos. El objetivo general fue analizar el impacto de estos delitos en la economía empresarial ecuatoriana, incluyendo la identificación de los delitos más comunes, el examen de la historia de la economía empresarial en el contexto de la digitalización y el análisis del marco legal existente. Para llevar a cabo la investigación, se empleó un enfoque cualitativo basado en la revisión bibliográfica y documental. Esta metodología permitió comprender la protección de datos en el sector empresarial ecuatoriano, así como las normativas vigentes relacionadas con los delitos informáticos. Los principales resultados alcanzados resaltaron la importancia de proteger los datos personales, evidenciando un aumento constante en los casos de delitos informáticos reportados. Se identificó que estas actividades ilegales no solo afectaron la integridad de los

[1] Universidad Estatal de Milagro, Ecuador
[2] Universidad Estatal de Milagro, Ecuador
[3] Universidad Estatal de Milagro, Ecuador
[4] Universidad Estatal de Milagro, Ecuador
[5] Universidad Estatal de Milagro, Ecuador
[6] Universidad Estatal de Milagro, Ecuador

Sinergia Académica ISSN: 2765-8252

Volumen: 7
Nro. 4
Año: 2024

Recepción: 08-07-2024 / Revisión: 13-09-2024 / Aprobación: 29-09-2024 / Publicación: 27-10-2024

datos, sino que también disminuyeron la confianza de los consumidores en las plataformas digitales, impactando negativamente la competitividad de las empresas, especialmente en el caso de las pequeñas y medianas empresas (pymes). La investigación subrayó la urgencia de implementar un marco legal y empresarial integral que fortalezca la ciberseguridad y proteja los datos en un entorno empresarial cada vez más digitalizado.

Abstract

The study addressed the problem of how cybercrime affected the business economy in Ecuador, highlighting the lack of adequate protection measures despite technological advances. The general objective was to analyze the impact of these crimes on the Ecuadorian business economy, including the identification of the most common crimes, the examination of the history of the business economy in the context of digitalization and the analysis of the existing legal framework. To carry out the research, a qualitative approach was used based on bibliographic and documentary review. This methodology allowed us to understand data protection in the Ecuadorian business sector, as well as current regulations related to computer crimes. The main results achieved highlighted the importance of protecting personal data, evidencing a constant increase in reported cases of computer crimes. It was identified that these illegal activities not only affected the integrity of the data, but also decreased consumer trust in digital platforms, negatively impacting the competitiveness of companies, especially in the case of small and medium-sized businesses (SMEs). The research underscored the urgency of implementing a comprehensive legal and business framework that strengthens cybersecurity and protects data in an increasingly digitalized business environment.

Palabras clave: delitos informáticos, ciberseguridad, economía empresarial, protección de datos

Keywords: computer crime, cybersecurity, business economics, data protection

Introducción

El impacto de los delitos informáticos en la economía empresarial del Ecuador se ha intensificado en los últimos años, impulsado por el crecimiento de la tecnología digital en los negocios. Estos delitos, que incluyen el robo de datos, fraudes electrónicos y ataques cibernéticos, afectan tanto a grandes corporaciones como a pequeñas y medianas empresas (pymes), generando pérdidas financieras y debilitando la confianza en las plataformas digitales. A pesar de los avances en el marco legal ecuatoriano, persisten desafíos en la protección efectiva contra estas amenazas. Este análisis integral busca explorar cómo los delitos informáticos inciden en el sector empresarial y examinar las respuestas legales y empresariales frente a esta problemática.

Según (Rendón, 2021) menciona que en la actualidad, el desarrollo y la expansión de las tecnologías de la información y comunicación (TIC) han transformado radicalmente el entorno

Sinergia Académica
ISSN: 2765-8252

Volumen: 7
Nro. 4
Año: 2024

Recepción: 08-07-2024 / Revisión: 13-09-2024 / Aprobación: 29-09-2024 / Publicación: 27-10-2024

empresarial a nivel mundial, y Ecuador no es la excepción. Por ende, la digitalización de procesos, el uso de plataformas electrónicas para el comercio y la adopción de sistemas informáticos avanzados han permitido a las empresas ecuatorianas ser más competitivas y eficientes. Sin embargo, este progreso también ha expuesto a las empresas a nuevos y complejos riesgos, siendo los delitos informáticos una de las amenazas más significativas. Estos delitos no solo comprometen la seguridad de la información, sino que también afectan la estabilidad económica, la confianza en el sistema financiero y la reputación de las organizaciones involucradas.

Los delitos informáticos abarcan toda actividad ilegal que utiliza las tecnologías de la información y la comunicación (TIC) como herramientas u objetivos. A nivel global, el término surgió a mediados de los años 70, con el aumento del uso de computadoras (Revista UNIR, 2024). En Ecuador, con la creciente dependencia de la tecnología, los delitos informáticos han afectado a empresas de todos los sectores, desde pequeñas y medianas empresas (PYMES) hasta grandes corporaciones.

Los ciberdelincuentes aprovechan vulnerabilidades en sistemas informáticos para sustraer información confidencial y utilizarla con fines maliciosos, tales como pedir rescates económicos o cometer fraudes financieros. Los principales ciberdelitos reconocidos a nivel mundial incluyen el malware, que infecta sistemas para alterar su funcionamiento; el ransomware, que secuestra información a cambio de rescates; el phishing, que engaña a usuarios haciéndose pasar por entidades legítimas para robar información, y el ciberacoso, que se refiere al acoso en línea y la difamación mediante el uso de la tecnología (Revista UNIR, 2024).

Normativa Legal en Ecuador

El derecho a la seguridad de la información en Ecuador está garantizado por la Constitución. En su artículo 66.19, se destaca la protección de la privacidad y los datos personales. La reciente Ley de Protección de Datos Personales (2021) también fortalece la seguridad de la información en empresas, exigiendo medidas técnicas y organizativas para proteger los datos personales, lo que incluye evitar accesos no autorizados. La protección de los datos y la seguridad de la información en Ecuador están respaldadas principalmente por la Constitución de la República del Ecuador y el Código Orgánico Integral Penal (COIP). La Constitución, en su artículo 66, numeral 19, garantiza el derecho a la intimidad y la protección de los datos personales, estableciendo que el Estado debe proteger los datos almacenados en bases públicas o privadas, así como sancionar cualquier violación a la intimidad.

Problema de investigación

Magali Paulina Coello Peralta
Marcelo Xavier Godoy Heredia
Christian Marcelo Taco Barragán
Diego Marcelo Villamarin Irazábal
Enrique Colon Ferruzola Gómez
Holguer Estuardo Romero Urréa
Sinergia Académica
ISSN: 2765-8252
Volumen: 7
Nro. 4
Año: 2024
Recepción: 08-07-2024 / Revisión: 13-09-2024 / Aprobación: 29-09-2024 / Publicación: 27-10-2024

El problema central que aborda este artículo es cómo los delitos informáticos están afectando la economía empresarial en Ecuador. A pesar del crecimiento tecnológico y la adopción de nuevas herramientas digitales, muchas empresas ecuatorianas no cuentan con las medidas necesarias para protegerse de estas amenazas. La pregunta clave es: ¿De qué manera los delitos informáticos están impactando a las empresas en Ecuador y cómo responde el marco legal vigente a esta problemática?

Objetivo de la investigación: Ofrecer un análisis integral sobre el impacto de los delitos informáticos en la economía empresarial del Ecuador, con un enfoque en los siguientes objetivos específicos.

- Identificar los tipos más comunes de delitos informáticos que afectan a las empresas ecuatorianas, evaluando sus implicaciones económicas y su frecuencia.
- Examinar la historia de la economía empresarial en Ecuador y cómo la digitalización ha contribuido tanto a la expansión económica como a la vulnerabilidad frente a ciberataques.
- Analizar el marco legal ecuatoriano vigente en relación con los delitos informáticos, evaluando su efectividad y sus limitaciones frente a la creciente sofisticación de los ataques.

Justificación

La importancia de esta investigación radica en la creciente dependencia de las empresas ecuatorianas de las tecnologías digitales, lo que las expone a riesgos cada vez más complejos y costosos. Según menciona el Diario El Comercio (2022), los delitos informáticos no solo representan una amenaza para la integridad de los datos empresariales, sino que también afectan la confianza de los consumidores y la competitividad de las empresas a nivel global. En un entorno donde la ciberseguridad se ha convertido en una prioridad, es fundamental entender cómo las empresas ecuatorianas están respondiendo a estas amenazas y qué mejoras son necesarias para proteger sus activos digitales.

Materiales y métodos

La investigación siguió un enfoque cualitativo, basado en una revisión bibliográfica y documental, lo que permitió una exploración detallada y una mejor comprensión de la protección de datos en el sector salud en Ecuador. Para alcanzar los objetivos establecidos, se emplearon una variedad de métodos, técnicas e instrumentos (Tabla 1).

Magali Paulina Coello Peralta
Marcelo Xavier Godoy Heredia
Christian Marcelo Taco Barragán
Diego Marcelo Villamarin Irazábal
Enrique Colon Ferruzola Gómez
Holguer Estuardo Romero Urréa
Sinergia Académica
ISSN: 2765-8252
Volumen: 7
Nro. 4
Año: 2024
Recepción: 08-07-2024 / Revisión: 13-09-2024 / Aprobación: 29-09-2024 / Publicación: 27-10-2024

Tabla 1. Enfoque de la investigación

Aspecto	Descripción
Enfoque de la investigación	Cualitativo, de tipo revisión bibliográfica y documental, centrado en el análisis de sentencias de la Corte Constitucional del Ecuador sobre delitos informáticos y protección de datos personales.
Objetivo del enfoque	Examinar las normativas y principios legales en el contexto ecuatoriano, junto con la interpretación judicial de estos principios.

Fuente: Elaboración propia (2024)

Tabla 2. Métodos utilizados

Métodos utilizados	Descripción
Análisis de jurisprudencia	Se examinó la jurisprudencia relacionada con delitos informáticos y la protección de datos personales a través de decisiones judiciales emitidas por la Corte Constitucional.
Análisis comparativo	Comparación de resoluciones judiciales para identificar tendencias y divergencias en la aplicación de la ley, con enfoque en el impacto sobre los derechos fundamentales.

Fuente: Elaboración propia (2024)

Tabla 3. Técnicas utilizadas

Técnicas utilizadas	Descripción
Revisión de jurisprudencia	Revisión exhaustiva de casos significativos, especialmente del Caso 0018-18-EP y el Caso 2062-20-EP, para identificar principios y criterios legales.
Análisis crítico	Evaluación detallada de las implicaciones de las decisiones judiciales en relación con la protección de datos y la intimidad.

Magali Paulina Coello Peralta
Marcelo Xavier Godoy Heredia
Christian Marcelo Taco Barragán
Diego Marcelo Villamarin Irazábal
Enrique Colon Ferruzola Gómez
Holguer Estuardo Romero Urréa
Sinergia Académica
ISSN: 2765-8252
Volumen: 7
Nro. 4
Año: 2024
Recepción: 08-07-2024 / Revisión: 13-09-2024 / Aprobación: 29-09-2024 / Publicación: 27-10-2024

Tabla 4. Instrumentos utilizados

Instrumentos utilizados	Descripción
Documentos jurídicos	Sentencias emitidas por la Corte Constitucional del Ecuador, utilizadas para analizar el marco normativo y la jurisprudencia sobre delitos informáticos.
Fuentes bibliográficas	Documentación académica y legal sobre protección de datos y delitos informáticos, que complementó el análisis de las decisiones judiciales.

Fuente: Elaboración propia (2024)

Resultados

Los resultados de la investigación destacan un enfoque teórico que subraya la relevancia de proteger los datos personales en el ámbito médico. La propuesta se enfoca en fortalecer las medidas de seguridad y confidencialidad en las historias clínicas electrónicas, basándose en los hallazgos obtenidos. En las tablas 5 y 6 se detallan el proceso aplicado y los casos analizados.

Tabla 5. Análisis de casos estudiados

Caso	Tipo de delito	Decisión de la corte	Implicaciones en derechos personales
Caso 0018-18-EP	Acceso no consentido a un sistema informático	Se ratificó la inocencia del acusado, destacando el derecho al debido proceso	Refuerza el principio de no culpabilidad y el respeto a la intimidad
Caso 2062-20-EP	Acceso no consentido a un sistema informático	Inadmite la acción extraordinaria de protección presentada	Subraya la importancia de una argumentación clara para la protección de derechos

Magali Paulina Coello Peralta
Marcelo Xavier Godoy Heredia
Christian Marcelo Taco Barragán
Diego Marcelo Villamarin Irazábal
Enrique Colon Ferruzola Gómez
Holguer Estuardo Romero Urréa
Sinergia Académica
ISSN: 2765-8252
Volumen: 7
Nro. 4
Año: 2024
Recepción: 08-07-2024 / Revisión: 13-09-2024 / Aprobación: 29-09-2024 / Publicación: 27-10-2024

Tabla 6. Estadísticas de delitos informáticos en Ecuador

Año	Total, de Delitos Informáticos	Acceso No Consentido	Fraude Informático	Suplantación de Identidad	Delitos contra la Propiedad Intelectual
2018	1,5	600	500	250	150
2019	2	700	800	300	200
2020	2,5	800	1	400	300
2021	3	1	1,2	500	400
2022	3,5	1,2	1,5	600	500
2023	4	1,5	1,8	700	600

Fuente: INEC (2024).

Propuesta

Para impulsar el cumplimiento del objetivo de ofrecer un análisis integral sobre el impacto de los delitos informáticos en la economía empresarial del Ecuador, se propone una estrategia que integre acciones tanto a nivel legal como empresarial y educativo. A continuación, se describen los componentes clave de la propuesta.

1. Fortalecimiento del marco legal y regulatorio.

El marco jurídico ecuatoriano debe actualizarse y robustecerse para enfrentar eficazmente los desafíos que presentan los delitos informáticos. Se recomienda una revisión exhaustiva del Código Orgánico Integral Penal (COIP) y otras normativas relacionadas, con el fin de incorporar sanciones más específicas y medidas preventivas para delitos cibernéticos. Además, es necesario crear incentivos fiscales para que las empresas, especialmente las pequeñas y medianas (pymes), inviertan en tecnologías de ciberseguridad y cumplan con las normativas de protección de datos.

2. Creación de un organismo especializado en ciberseguridad empresarial.

Una entidad nacional, compuesta por expertos en seguridad informática, autoridades gubernamentales y representantes del sector privado, debe coordinar y supervisar la implementación de medidas de ciberseguridad en el país. Este organismo puede brindar asesoría técnica a empresas, ofrecer certificaciones de buenas prácticas y asegurar la creación de un entorno colaborativo entre empresas y gobierno para compartir información sobre posibles amenazas y soluciones a ciberataques.

Magali Paulina Coello Peralta
Marcelo Xavier Godoy Heredia
Christian Marcelo Taco Barragán
Diego Marcelo Villamarin Irazábal
Enrique Colon Ferruzola Gómez
Holguer Estuardo Romero Urréa
Sinergia Académica
ISSN: 2765-8252
Volumen: 7
Nro. 4
Año: 2024
Recepción: 08-07-2024 / Revisión: 13-09-2024 / Aprobación: 29-09-2024 / Publicación: 27-10-2024

3. Implementación de programas de capacitación y sensibilización

Un componente clave para reducir el impacto de los delitos informáticos es la educación empresarial en ciberseguridad. Se debe implementar un programa nacional de capacitación para empleados y directivos de empresas, especialmente pymes, con el objetivo de mejorar las prácticas de protección de datos y seguridad digital. Este programa puede ser impulsado por el Ministerio de Telecomunicaciones, en conjunto con cámaras de comercio y asociaciones empresariales, con enfoque en riesgos cibernéticos, protección de información sensible y respuesta ante incidentes.

4. Desarrollo de infraestructura tecnológica accesible para las pymes

Dado que muchas empresas en Ecuador carecen de los recursos para implementar tecnologías de seguridad avanzadas, se propone fomentar la creación de plataformas y soluciones tecnológicas accesibles y económicas que ayuden a proteger los sistemas de información empresarial. Esto puede incluir la colaboración entre el sector privado y universidades para el desarrollo de software de seguridad básico o servicios de monitoreo a precios reducidos, accesibles para las pymes.

5. Fomento de alianzas internacionales en materia de ciberseguridad

El Ecuador debe fortalecer sus relaciones internacionales en materia de ciberseguridad, especialmente con países que han logrado avances significativos en la prevención de delitos informáticos. Estas alianzas pueden facilitar el intercambio de conocimientos, acceso a tecnología de punta y formación de equipos especializados que monitoreen amenazas a nivel global. Participar en iniciativas regionales y globales permitirá a las empresas ecuatorianas adoptar mejores prácticas y mantenerse actualizadas sobre las nuevas amenazas en el entorno digital.

6. Creación de un fondo de emergencia para la respuesta rápida a ciberataques

Para mitigar las pérdidas económicas derivadas de delitos informáticos, se sugiere establecer un fondo de emergencia destinado a empresas afectadas por ciberataques. Este fondo podría financiarse a través de contribuciones del sector privado y público, y estaría destinado a ofrecer soporte inmediato a las empresas en la recuperación de sus operaciones, adquisición de herramientas de protección y análisis forense posataque.

7. Incentivos para la innovación en ciberseguridad empresarial

Finalmente, se propone crear un programa de incentivos para empresas y startups que desarrollen soluciones innovadoras en el ámbito de la ciberseguridad. Estas iniciativas tecnológicas no solo

Sinergia Académica
ISSN: 2765-8252

Volumen: 7
Nro. 4
Año: 2024

Recepción: 08-07-2024 / Revisión: 13-09-2024 / Aprobación: 29-09-2024 / Publicación: 27-10-2024

contribuirían a la protección de las empresas locales, sino que también podrían posicionar a Ecuador como un centro de innovación en seguridad informática a nivel regional.

Implementar estas acciones ofrecerá un marco integral para abordar el impacto de los delitos informáticos en la economía empresarial de Ecuador, contribuyendo a la seguridad digital y a la sostenibilidad de las empresas en un entorno cada vez más digitalizado.

Discusión

La investigación se llevó a cabo mediante una revisión bibliográfica y documental, con un enfoque cualitativo que permitió analizar en profundidad las sentencias emitidas por la Corte Constitucional del Ecuador relacionadas con delitos informáticos y la protección de datos personales. Este enfoque facilitó la identificación de normativas y principios legales que rigen la materia, así como la interpretación judicial de estos principios en contextos específicos. En el marco de la metodología aplicada, se realizó una exhaustiva revisión de la jurisprudencia pertinente, centrándose en los casos más destacados, especialmente el Caso 0018-18-EP y el Caso 2062-20-EP. Estos casos resultaron significativos, ya que no solo abordaron la legalidad del acceso no consentido a sistemas informáticos, sino que también establecieron precedentes en cuanto a los derechos fundamentales involucrados. Se identificaron criterios y principios en las sentencias que reflejaron la posición del tribunal respecto a cuestiones de acceso a datos y la protección de la intimidad.

El análisis comparativo de las resoluciones permitió evidenciar tendencias y divergencias en la aplicación de la ley. Se observó que, a pesar de la variabilidad en las decisiones judiciales en función de los contextos y las circunstancias de cada caso, hubo un enfoque común en la defensa de los derechos a la intimidad y a la protección de datos personales. Este aspecto fue particularmente relevante, ya que las decisiones del tribunal reflejaron una evolución en la jurisprudencia que intentó equilibrar el derecho a la privacidad con la necesidad de investigar y sancionar delitos informáticos. A su vez, se examinó el impacto de las decisiones sobre los derechos fundamentales de los individuos. En el Caso 0018-18-EP, la Corte ratificó la inocencia del acusado, destacando la importancia del debido proceso y reforzando el principio de no culpabilidad. En contraste, en el Caso 2062-20-EP, la acción extraordinaria de protección fue inadmitida, lo que subrayó la necesidad de una argumentación clara para garantizar la protección de derechos en el contexto de los delitos informáticos. Estas decisiones reflejaron una interpretación cuidadosa de la normativa ecuatoriana, que busca asegurar el respeto a los derechos humanos en un ámbito cada vez más digitalizado.

En relación con las estadísticas de delitos informáticos en Ecuador, se constató un aumento constante en la cantidad total de delitos reportados a lo largo de los años, desde 1,500 en 2018 hasta 4,000 en 2023. Este crecimiento podría atribuirse tanto a un incremento real en la

Sinergia Académica
ISSN: 2765-8252

Volumen: 7
Nro. 4
Año: 2024

Recepción: 08-07-2024 / Revisión: 13-09-2024 / Aprobación: 29-09-2024 / Publicación: 27-10-2024

incidencia de estos delitos como a una mejora en la capacidad de reporte y registro por parte de las autoridades competentes. El análisis de los tipos de delitos más comunes reveló que el acceso no consentido a sistemas informáticos se posicionó como el delito más reportado, con un aumento significativo que pasó de 600 casos en 2018 a 1,500 en 2023. El fraude informático también mostró un crecimiento notable, con un incremento de 500 a 1,800 casos en el mismo periodo. La suplantación de identidad y los delitos contra la propiedad intelectual, aunque menos frecuentes, también evidenciaron un aumento, reflejando la creciente sofisticación de las técnicas utilizadas por los delincuentes en el ámbito digital.

Este incremento en la incidencia de delitos informáticos subraya la necesidad urgente de implementar políticas más efectivas de prevención y respuesta. A medida que el uso de la tecnología se expande en Ecuador, también lo hace la vulnerabilidad de las infraestructuras digitales y la información personal. La normativa ecuatoriana, en su búsqueda de proteger los derechos fundamentales, deberá adaptarse a esta realidad, promoviendo un marco legal que contemple no solo la sanción de delitos, sino también la educación y la concienciación de la población sobre la importancia de la ciberseguridad. En conclusión, el análisis de la metodología aplicada en la investigación y las estadísticas encontradas acerca de los delitos cibernéticos en Ecuador proporcionan una visión comprensiva del estado actual de la jurisprudencia y la normativa en el país. La interacción entre las decisiones judiciales y las estadísticas de delitos informáticos revela no solo la evolución de la jurisprudencia, sino también la urgencia de una respuesta adecuada por parte del sistema legal ecuatoriano ante un fenómeno que continúa creciendo en complejidad y alcance.

Conclusiones

Los delitos informáticos han generado un aumento considerable en las vulnerabilidades empresariales dentro del Ecuador, afectando tanto a grandes corporaciones como a pequeñas y medianas empresas (pymes). Este impacto se manifiesta principalmente en las empresas que dependen de la tecnología digital para sus operaciones cotidianas. Las pymes, debido a sus limitaciones económicas y a la falta de conocimientos especializados en ciberseguridad, son particularmente susceptibles a estos riesgos, lo que pone en peligro la sostenibilidad de sus negocios en el entorno digital actual.

El impacto financiero de los delitos informáticos en las empresas ecuatorianas es significativo. La creciente incidencia de fraudes, ataques cibernéticos y robo de información ha causado pérdidas económicas directas, ya sea por el pago de rescates en casos de ransomware o por los costos asociados a la recuperación de datos y la restauración de operaciones. Además, las empresas afectadas experimentan una pérdida de confianza por parte de sus clientes y socios comerciales,

Sinergia Académica
ISSN: 2765-8252

Volumen: 7
Nro. 4
Año: 2024

Recepción: 08-07-2024 / Revisión: 13-09-2024 / Aprobación: 29-09-2024 / Publicación: 27-10-2024

lo que se traduce en una disminución de ingresos a largo plazo, afectando gravemente la estabilidad de sus negocios.

A pesar de los avances legislativos en Ecuador, como la tipificación de los delitos informáticos en el Código Orgánico Integral Penal (COIP), las normativas actuales presentan limitaciones en su alcance y efectividad. La falta de personal capacitado para enfrentar estos delitos, así como la complejidad inherente a los crímenes digitales, dificulta una aplicación eficiente de la normativa. Esto refleja una necesidad urgente de fortalecer el marco jurídico y mejorar los mecanismos de respuesta ante los delitos informáticos en el país.

Es evidente que la prevención de los delitos informáticos en el ámbito empresarial ecuatoriano requiere un enfoque integral. Las empresas deben adoptar medidas proactivas, invirtiendo en infraestructura tecnológica más segura y en la capacitación continua de sus empleados para prevenir ataques cibernéticos. La educación digital juega un papel clave en este aspecto, ya que las buenas prácticas en el uso de herramientas digitales son esenciales para minimizar los riesgos y mejorar la protección de los activos empresariales.

Finalmente, la colaboración entre el sector público y el privado es fundamental para mitigar el impacto de los delitos informáticos en la economía empresarial. La creación de alianzas estratégicas y el intercambio de información sobre amenazas cibernéticas permitiría una mejor gestión y respuesta ante incidentes. Asimismo, una mayor intervención del Estado, mediante políticas de ciberseguridad más robustas, resultaría crucial para proteger el ecosistema empresarial del país frente a los crecientes desafíos del entorno digital.

Referencias

Bueno, G. & Haz, L. (2022). Ciberseguridad post Covid-19 y su impacto en las pymes del Ecuador. *Revista De Producción, Ciencias E Investigación, 6*(46), 103-120. https://doi.org/10.29018/issn.2588-1000vol6iss46.2022pp103-120

Desafíos y respuestas legales ante los delitos informáticos en Ecuador. (2024). *Revista San Gregorio, 1*(58), 111-118. http://scielo.senescyt.gob.ec/scielo.php?script=sci_arttext&pid=S2528-79072024000200111

Diario El Comercio. (2022, 25 de julio). Delitos informáticos que se han registrado en el Ecuador. https://www.elcomercio.com/actualidad/seguridad/3183-delitos-informaticos-se-han-

Esg Innova. (2021). *¿Qué es la seguridad de la información y cuantos tipos hay*? https://www.pmg-ssi.com/2021/03/que-es-la-seguridad-

Sinergia Académica ISSN: 2765-8252

Volumen: 7
Nro. 4
Año: 2024

Recepción: 08-07-2024 / Revisión: 13-09-2024 / Aprobación: 29-09-2024 / Publicación: 27-10-2024

Fiscala General del Estado. (2023). *Fiscalía obtiene sentencia por los delitos de acceso no.* https://www.fiscalia.gob.ec/fiscalia-obtiene-sentencia-por-los-delitos-de-

Inconstitucionalidad presentada en contra del Reglamento para el Subsistema de Interceptación de Comunicaciones o Datos Informáticos. *CASO No. 77-16-IN* (2022, 27 de enero). http://esacc.corteconstitucional.gob.ec/storage/api/v1/10_DWL_FL/e2NhcnBldGE6J3

Inec. (2024). *Tecnologías de la Información y Comunicación*. INEC.

iTahora. (2024). ¡*Es momento de elevar la Ciberseguridad en las PYMES en Ecuador!* iTahora. https://itahora.com/2024/04/22/es-momento-de-elevar-la-ciberseguridad-en-las-pymes-en-ecuador/

iTahora. (2024). *La ciberseguridad en Ecuador: La vulnerabilidad del periodismo en el espacio digital*. iTahora.

Juca, F. (2023). Ciberdelitos en Ecuador y su impacto social; panorama actual y futuras. *Revista Portal de la Ciencia, 4*(3), 325-337. https://doi.org/10.51247/pdlc.v4i3.394

Mezones-Santana, J. J.-U. (2022). Valoración de la filosofía de economía circular en una producción avícola de Ecuador. Ingeniería Industrial. *Revista Scielo, 43*(2), 90-98. http://scielo.sld.cu/scielo.php?pid=S1815-59362022000200090&script=sci_arttext&tlng=pt

Ministerio de Telecomunicaciones. (2021). El ministro de telecomunicaciones y de la sociedad de la información (S). https://www.telecomunicaciones.gob.ec/wp-content/uploads/2021/06/Acuerdo-No.-006-2021-Politica-de-Ciberseguridad.pdf

Ministerio de Telecomunicaciones y de la Sociedad de la Información. (2023). *El 82,3% de Mipymes en el Ecuador utilizan Internet.* https://www.telecomunicaciones.gob.ec/el-823-de-mipymes-en-el-ecuador-utilizan-internet/

Ortiz, N. (2019). Normativa Legal sobre Delitos Informáticos en Ecuador. *Revista Hallazgos*, 21, 100-111. Obtenido de https://revistas.pucese.edu.ec/hallazgos21/article/view/336

Ponce, M. (2024). Delitos informáticos: Caso Ecuador. *Revista San Gregorio, 1*(58), 119-123. https://doi.org/10.36097/rsan.v1i58.2667

Pulles, A. (2023). Tecnologías de la información y comunicación en Ecuador. *Revista DOXA, 1*(1), 1-4. https://itq.edu.ec/wp-content/uploads/2023/06/2023-03-

Sinergia Académica ISSN: 2765-8252

Volumen: 7
Nro. 4
Año: 2024

Recepción: 08-07-2024 / Revisión: 13-09-2024 / Aprobación: 29-09-2024 / Publicación: 27-10-2024

Quizhpe, D. (2022). Incidencia de las TIC sobre la expansión económica en Ecuador: Un enfoque hacia el desarrollo sostenible. *Revista Económica, 10*(2), 96-112. https://doi.org/10.54753/rve.v10i2.1409

Rendón, A. (2021). Delitos informáticos en tiempos de Covid: revisión literaria Ecuador. *Revista Literaria Ecuador*, 1-15. https://www.espam.edu.ec/recursos/sitio/informativo/archivos/ponencias/vinculacion/i

Revista Unir. (2024). *¿Qué son los delitos informáticos o ciberdelitos?* https://ecuador.unir.net/actualidad-unir/delitos-informaticos/

Saltos, M. F., Robalino, J. L., & Pazmiño, L. D. (2021). Análisis conceptual del delito en Ecuador. *Revista Conrada, 17*(78), 343-351.

Saltos, M. (2021). Análisis conceptual del delito informático en Ecuador. *Revista Scielo, 17*(78), 343-351. http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S1990-86442021000100343

Toala, Y. (2021). Delitos informáticos frecuentes en el Ecuador: casos de estudio. http://dspace.ups.edu.ec/handle/123456789/20942