Sinergia Académica
ISSN: 2765-8252

Volumen: 7.
Nro. Especial 5
Año: 2024

Recepción: 07-06-2024 / Revisión: 10-07-2024 / Aprobación: 15-08-2024 / Publicación: 27-08-2024

La ciberdelincuencia y la protección de datos personales

Cybercrime and personal data protection

Carlos Javier Bazurto Mecias[1] (cbazurtom3@unemi.edu.ec) (https://orcid.org/0009-0003-1533-023X)

Yulexi Katherine Jurado Cabello[2] (yjuradoc@unemi.edu.ec) (https://orcid.org/0009-0009-4938-239X)

Luz Maria Sifa Mueses[3] (lsifam@unemi.edu.ec) (https://orcid.org/0009-0007-4576-3983)

Alejandra Gabriela Reinoso Paredes[4] (areinosop2@unemi.edu.ec) (https://orcid.org/0009-0003-2436-5258)

Resumen

La ciberdelincuencia ha experimentado un crecimiento significativo en la era digital, afectando a individuos y organizaciones a nivel global. Este artículo analiza la protección de datos personales y los desafíos jurídicos asociados en Ecuador, enmarcados en la Constitución de 2008 y la Ley Orgánica de Protección de Datos Personales de 2021. A través de un análisis detallado de las diversas formas de ciberdelincuencia, como el acceso ilícito, el fraude informático y la distribución de contenido ilegal, se examina el impacto de estas actividades en la privacidad y seguridad de los datos. Además, se abordan las dificultades que enfrentan las autoridades en la aplicación de leyes debido a la criptografía y la anonimización de datos, así como el uso de Blockchain y criptomonedas en actividades ilícitas. El artículo también discute el aumento de los delitos cibernéticos en Ecuador, ilustrado por el caso Ola Bini, y el papel de la inteligencia artificial y el Big Data en la privacidad. Finalmente, se resaltan las estrategias de ciberseguridad necesarias en el sector financiero para proteger los datos sensibles y garantizar la estabilidad económica.

[1] Universidad Estatal de Milagro (UNEMI), Ecuador
[2] Universidad Estatal de Milagro (UNEMI), Ecuador.
[3] Universidad Estatal de Milagro (UNEMI), Ecuador.
[4] Universidad Estatal de Milagro (UNEMI), Ecuador.

Sinergia Académica
ISSN: 2765-8252

Volumen: 7.
Nro. Especial 5
Año: 2024

Recepción: 07-06-2024 / Revisión: 10-07-2024 / Aprobación: 15-08-2024 / Publicación: 27-08-2024

Palabras clave: ciberdelincuencia, protección de datos personales, ciberseguridad.

Abstract

In the digital age, information has become a highly valuable asset, attracting not only individuals and companies but also criminals seeking to exploit it for illicit purposes. Cybercrime, defined as any criminal activity involving the use of computer technology and communication networks, has experienced exponential growth in recent years. This article explores the protection of personal data in the context of cybercrime, focusing on Ecuador's legal framework established by the 2008 Constitution and the 2021 Organic Law on Personal Data Protection. The article provides a comprehensive analysis of various forms of cybercrime, such as unauthorized access, computer fraud, and the distribution of illegal content, examining their impact on data privacy and security. It also addresses the challenges faced by authorities in enforcing laws due to encryption and data anonymization, as well as the use of blockchain and cryptocurrencies in illicit activities. The increasing incidence of cybercrime in Ecuador, exemplified by the Ola Bini case, is discussed alongside the role of artificial intelligence and Big Data in privacy concerns. The article concludes by highlighting necessary cybersecurity strategies in the financial sector to protect sensitive data and ensure economic stability.

Key words: cybercrime - personal data protection - cybersecurity.

Introducción

En la era digital, la información se ha convertido en uno de los activos más valiosos, no solo para individuos y empresas, sino también para delincuentes que buscan explotarla con fines ilícitos. La ciberdelincuencia, definida como cualquier actividad delictiva que involucra el uso de tecnología informática y redes de comunicación, ha experimentado un crecimiento exponencial en los últimos años.

La protección de datos personales se erige como un componente importante en este contexto, ya que los datos constituyen el objetivo principal de muchos ciberataques. En Ecuador, la Constitución de la República de 2008 y la Ley Orgánica de Protección de Datos Personales,

Sinergia Académica
ISSN: 2765-8252

Volumen: 7.
Nro. Especial 5
Año: 2024

Recepción: 07-06-2024 / Revisión: 10-07-2024 / Aprobación: 15-08-2024 / Publicación: 27-08-2024

promulgada en 2021, establecen el marco jurídico nacional para la protección de la información personal. Complementariamente, el Código Orgánico Integral Penal (COIP), en sus artículos 178 y 229, tipifica y sanciona los delitos relacionados con la violación de la intimidad y la manipulación de datos informáticos.

La ciberdelincuencia no solo incluye actos de intrusión y robo de datos, sino también la manipulación de información, el sabotaje cibernético y el fraude digital, entre otros. Estas actividades ilícitas no solo comprometen la privacidad de los individuos, sino que también pueden causar daños económicos y poner en riesgo la seguridad nacional. En este sentido, en el ámbito jurídico enfrenta el reto de tipificar adecuadamente estos delitos y establecer mecanismos efectivos para su prevención y sanción.

Históricamente, la evolución tecnológica ha superado en muchas ocasiones la capacidad de respuesta legislativa, creando vacíos legales que son explotados por los ciberdelincuentes. A su vez, la cooperación internacional se torna indispensable, dado el carácter transnacional de muchos de estos delitos. Organismos como Interpol y Europol son fundamentales en la coordinación de esfuerzos para combatir la ciberdelincuencia a nivel global.

Materiales y métodos

Para la elaboración de este artículo se emplearon métodos cualitativos y cuantitativos que permiten una comprensión integral de la ciberdelincuencia y la protección de datos personales. En el ámbito cualitativo, se llevó a cabo una revisión exhaustiva de la literatura académica que incluye libros, artículos científicos, y estudios de caso recientes. Este enfoque permitió analizar los enfoques teóricos y doctrinales sobre la ciberdelincuencia, así como las respuestas legales y tecnológicas actuales. Adicionalmente, se revisaron informes de ciberseguridad tanto nacionales como internacionales, que proporcionaron un panorama detallado sobre las tendencias emergentes y las mejores prácticas en la protección de datos personales.

En el ámbito cuantitativo, se analizaron datos estadísticos obtenidos de fuentes clave como la Asociación Ecuatoriana de Ciberseguridad, la Policía Nacional de Ecuador, y otros informes relevantes. Este análisis incluyó la recopilación y evaluación de datos sobre la incidencia y

Recepción: 07-06-2024 / Revisión: 10-07-2024 / Aprobación: 15-08-2024 / Publicación: 27-08-2024

evolución de los delitos cibernéticos en el país, empleando técnicas estadísticas avanzadas para interpretar las tendencias y patrones observados. La combinación de estos métodos permitió una evaluación rigurosa y completa de la situación actual de la ciberdelincuencia en Ecuador, así como de las medidas de protección de datos personales implementadas en respuesta a esta problemática, en materia de derecho penal.

Resultados

Definición y clasificación de los delitos cibernéticos

Los delitos cibernéticos, también conocidos como ciberdelitos, se refieren a cualquier actividad delictiva que se lleva a cabo utilizando tecnologías de la información y la comunicación (TIC). Estas actividades pueden afectar tanto a individuos como a organizaciones, y abarcan una amplia gama de conductas ilícitas. La siguiente clasificación proporciona una visión estructurada de los principales tipos de delitos cibernéticos.

Delitos contra la confidencialidad, integridad y disponibilidad de los datos

Estos delitos se centran en el acceso no autorizado, la alteración y la destrucción de datos, sistemas informáticos o redes, comprometiendo su confidencialidad, integridad y disponibilidad. Entre ellos se encuentran los siguientes.

Acceso ilícito: consiste en la intrusión en sistemas informáticos sin autorización, comúnmente conocido como hacking. En el COIP, este tipo de delito está tipificado en el artículo 234, que sanciona el acceso no consentido a sistemas informáticos.

- El informe de la Policía Nacional de Ecuador sobre delitos cibernéticos del 2021 registró más de 3,500 casos de acceso no autorizado a sistemas informáticos (Policía Nacional de Ecuador, 2021).
- En 2022, el Ministerio del Interior reportó que los delitos de acceso ilícito a sistemas informáticos aumentaron en un 20% en comparación con el año anterior (Ministerio del Interior, 2022).

Sinergia Académica
ISSN: 2765-8252

Volumen: 7.
Nro. Especial 5
Año: 2024

Recepción: 07-06-2024 / Revisión: 10-07-2024 / Aprobación: 15-08-2024 / Publicación: 27-08-2024

Intercepción ilícita: implica la interceptación de comunicaciones privadas sin permiso, vulnerando la privacidad de los individuos (Artículo 230 del COIP).

- Según datos del Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL), hubo más de 1,200 casos de intercepción ilícita de comunicaciones reportados en 2022 (Ministerio de Telecomunicaciones y de la Sociedad de la Información, 2022).
- La Superintendencia de Telecomunicaciones registró un incremento del 15% en las denuncias por intercepción ilegal de comunicaciones en el último año (2022).
- Daño a datos y sistemas informáticos: incluye la destrucción, alteración, supresión o deterioro de datos, programas informáticos o sistemas informáticos. Este delito está regulado en el artículo 235 del COIP.
- El informe de ARCOTEL del 2022 identificó más de 2,000 incidentes de destrucción, alteración o daño a sistemas informáticos (2022).
- La Fiscalía General del Estado indicó que los delitos de daño a datos y sistemas informáticos representan el 18% del total de delitos informáticos reportados en 2021.
- Ataques de denegación de servicio (DDoS): se refiere a la interrupción de servicios a usuarios legítimos mediante la sobrecarga de sistemas o redes.
- El ECU-CERT reportó más de 500 incidentes de ataques DDoS en 2022, con un aumento del 30% respecto al año anterior (Centro de Respuesta a Incidentes Informáticos del Ecuador, 2022).
- Empresas del sector financiero y gubernamental fueron las más afectadas, con un 60% de los ataques dirigidos a estas entidades.

Incidencia de delitos informáticos: según el Informe de Seguridad Digital en Ecuador de la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL) del 2022, hubo un aumento significativo en los delitos informáticos, con más de 10,000 incidentes reportados anualmente

- El Centro de Respuesta a Incidentes Informáticos del Ecuador (ECU-CERT) informó un incremento del 25% en ataques cibernéticos durante el último año (2022).

Sinergia Académica
ISSN: 2765-8252

Volumen: 7.
Nro. Especial 5
Año: 2024

Recepción: 07-06-2024 / Revisión: 10-07-2024 / Aprobación: 15-08-2024 / Publicación: 27-08-2024

Fraudes informáticos

Los fraudes informáticos representan una amplia gama de actividades fraudulentas que utilizan tecnologías de la información para cometer estafas y obtener beneficios económicos de manera ilícita. Estos delitos no solo causan pérdidas financieras, sino que también pueden comprometer la seguridad y la privacidad de las personas y organizaciones. A continuación, se detallan algunos de los tipos más comunes de fraudes informáticos.

- Phishing: es una técnica utilizada para engañar a los usuarios y obtener información confidencial, como contraseñas y datos bancarios, haciéndose pasar por una entidad de confianza. Los atacantes suelen enviar correos electrónicos falsificados que parecen provenir de instituciones legítimas, como bancos o servicios en línea, solicitando a los destinatarios que proporcionen sus credenciales de acceso. Según el "Informe sobre el Estado de la Ciberseguridad en Ecuador, 2023" de la Asociación Ecuatoriana de Ciberseguridad, los ataques de phishing representaron el 40% de los incidentes reportados en el último año, afectando a miles de usuarios en todo el país.
- Skimming: implica la clonación de tarjetas de crédito mediante dispositivos instalados en cajeros automáticos o terminales de puntos de venta. Estos dispositivos capturan la información de la tarjeta y el PIN cuando los usuarios realizan transacciones. Un estudio de la Policía Nacional del Ecuador indica que en 2022 se registraron más de 1,500 casos de Skimming, con pérdidas estimadas en millones de dólares. Este tipo de fraude no solo afecta a los usuarios individuales, sino también a las instituciones financieras que deben asumir los costos asociados a la reposición de tarjetas y reembolso de fondos.
- Ingeniería social: se refiere a la manipulación de personas para que revelen información confidencial o realicen acciones que comprometan la seguridad de los sistemas informáticos. Los atacantes pueden hacerse pasar por empleados de una empresa, técnicos de soporte o incluso amigos y familiares para engañar a sus víctimas. Según el "Reporte de Amenazas Globales 2023" de Kaspersky, los ataques de ingeniería social han aumentado en un 20% a nivel mundial, reflejando una tendencia similar en Ecuador, donde se reportaron numerosos

Sinergia Académica ISSN: 2765-8252

Volumen: 7.
Nro. Especial 5
Año: 2024

Recepción: 07-06-2024 / Revisión: 10-07-2024 / Aprobación: 15-08-2024 / Publicación: 27-08-2024

incidentes de este tipo que resultaron en el acceso no autorizado a sistemas corporativos y la filtración de datos sensibles.

Datos estadísticos y análisis

El impacto de los fraudes informáticos en la economía y la seguridad de la información ha sido significativo en los últimos años. A continuación, se presenta una tabla con datos estadísticos relevantes sobre el incremento de estos delitos en Ecuador.

Tabla 1. Datos estadísticos sobre fraudes informáticos en Ecuador.

Año	Incidentes de phishing reportados	Casos de skimming reportados	Incremento en ataques de ingeniería social (%)
2019	5,000	1,200	15%
2020	7,500	1,350	18%
2021	10,000	1,500	20%
2022	14,000	1,750	22%
2023	20,000	2,000	25%

Estos datos, recopilados de informes de la Asociación Ecuatoriana de Ciberseguridad y de la Policía Nacional del Ecuador, muestran un incremento sostenido en los incidentes de fraudes informáticos, lo que subraya la urgencia de implementar medidas de ciberseguridad más robustas y campañas de concienciación pública para mitigar estos riesgos.

Delitos relacionados con contenido ilícito

La creciente digitalización ha traído consigo un aumento importante en los delitos cibernéticos, los cuales abarcan una variedad de actividades ilícitas en el entorno digital. Estos delitos implican la creación, distribución o posesión de contenido ilegal que puede ser perjudicial para la sociedad. Entre ellos se encuentran los siguientes.

Sinergia Académica
ISSN: 2765-8252

Volumen: 7.
Nro. Especial 5
Año: 2024

Recepción: 07-06-2024 / Revisión: 10-07-2024 / Aprobación: 15-08-2024 / Publicación: 27-08-2024

Pornografía infantil

La producción, distribución y posesión de material pornográfico que involucra a menores es un grave delito tipificado en el artículo 103 del Código Orgánico Integral Penal (COIP). Este artículo establece lo siguiente.

> La persona que fotografíe, filme, grabe, produzca, transmita o edite materiales visuales, audiovisuales, informáticos, electrónicos o de cualquier otro soporte físico o formato que contenga la representación visual de desnudos o semidesnudos reales o simulados de niñas, niños o adolescentes en actitud sexual; será sancionada con pena privativa de libertad de trece a dieciséis años.

Además, se agravan las penas en situaciones donde la víctima sufra alguna discapacidad, enfermedad grave o incurable, o cuando el infractor tenga una relación de confianza o autoridad sobre la víctima, como en el caso de padres, tutores, maestros o ministros de culto, llegando hasta una pena privativa de libertad de veintidós a veintiséis años.

Terrorismo

El uso de Internet y otras tecnologías de la información y comunicación (TIC) para promover actividades terroristas, reclutar miembros o difundir propaganda extremista está sancionado en el artículo 366 del COIP. Este artículo especifica lo siguiente.

> La persona que individualmente o formando asociaciones armadas, provoque o mantenga en estado de terror a la población o a un sector de ella, mediante actos que pongan en peligro la vida, la integridad física o la libertad de las personas o pongan en peligro las edificaciones, medios de comunicación, transporte, valiéndose de medios capaces de causar estragos, será sancionada con pena privativa de libertad de diez a trece años.

Este artículo también detalla las penas para acciones específicas como el control ilegal de transportes, destrucción de infraestructuras críticas, actos de violencia en transportes públicos, difusión de informes falsos que pongan en peligro la seguridad pública, y financiación de

Recepción: 07-06-2024 / Revisión: 10-07-2024 / Aprobación: 15-08-2024 / Publicación: 27-08-2024

actividades terroristas. La pena máxima, que puede llegar hasta veintiséis años, se aplica cuando tales actos resultan en la muerte de una o más personas.

Discurso de odio y ciberacoso

El artículo 177 del COIP aborda la difusión de mensajes de odio, amenazas y acoso a través de plataformas digitales.

> La persona que cometa actos de violencia física o psicológica de odio, contra una o más personas en razón de su nacionalidad, etnia, lugar de nacimiento, edad, sexo, identidad de género u orientación sexual, identidad cultural, estado civil, idioma, religión, ideología, condición socioeconómica, condición migratoria, discapacidad, estado de salud o portar VIH, será sancionada con pena privativa de libertad de uno a tres años.

Las penas se agravan si los actos de violencia provocan heridas graves o la muerte de la víctima, en cuyo caso la sanción puede alcanzar hasta veintiséis años de privación de libertad.

Desafíos jurídicos en la era digital

La criptografía y la anonimización de datos son tecnologías esenciales para proteger la privacidad y la seguridad en el entorno digital. Sin embargo, también presentan desafíos para el marco jurídico.

Criptografía y la anonimización de datos

La criptografía es la práctica de codificar información de tal manera que solo pueda ser leída por personas autorizadas. Esta técnica es fundamental para asegurar la confidencialidad de las comunicaciones y proteger datos sensibles contra accesos no autorizados. Existen dos tipos principales de criptografía: simétrica y asimétrica. La criptografía simétrica utiliza una única clave para encriptar y desencriptar la información, siendo el *Advanced Encryption Standard* (AES) un ejemplo común. Por otro lado, la criptografía asimétrica emplea un par de claves, una pública y una privada, para encriptar y desencriptar datos, como en el caso del algoritmo RSA.

Sinergia Académica
ISSN: 2765-8252

Volumen: 7.
Nro. Especial 5
Año: 2024

Recepción: 07-06-2024 / Revisión: 10-07-2024 / Aprobación: 15-08-2024 / Publicación: 27-08-2024

En los últimos cinco años, el uso de técnicas avanzadas de criptografía ha aumentado exponencialmente. Según un informe de la Asociación Internacional de Investigación Criptológica (AIC), el uso de criptografía simétrica como el AES se ha consolidado como el estándar más implementado en aplicaciones comerciales, representando más del 70% de las implementaciones criptográficas en el ámbito empresarial a nivel mundial. Además, la criptografía asimétrica, particularmente RSA y ECC (criptografía de curva elíptica), ha visto un incremento significativo en su adopción debido a su eficacia en entornos donde la seguridad y la autenticación son importantes, especialmente en transacciones financieras y comunicaciones seguras.

De la misma forma, estos presentan desafíos para la investigación criminal y la aplicación de la ley. Uno de los principales problemas es el acceso a evidencia encriptada. Los delincuentes pueden utilizar cifrados avanzados para proteger sus comunicaciones y datos ilícitos, lo que dificulta su acceso por parte de las fuerzas del orden. La recolección y análisis de pruebas encriptadas requiere recursos técnicos avanzados y puede ralentizar las investigaciones. Según un informe del Europol de 2022, aproximadamente el 60% de las investigaciones criminales en Europa involucraron algún tipo de cifrado que dificultó el acceso a la evidencia, subrayando la creciente adopción de tecnologías de cifrado por parte de actores malintencionados.

Además, algunos gobiernos han propuesto la implementación de "puertas traseras" en sistemas de cifrado para permitir el acceso de las autoridades. Sin embargo, esto plantea riesgos para la seguridad y privacidad de los usuarios, ya que tales puertas traseras también podrían ser explotadas por ciberdelincuentes. Un estudio realizado por el Instituto de Ingenieros Eléctricos y Electrónicos (IEE), en 2021, indicó que la introducción de puertas traseras comprometería gravemente la integridad de los sistemas de cifrado, exponiendo a los usuarios a vulnerabilidades que podrían ser explotadas por atacantes con conocimientos avanzados.

Por otro lado, la anonimización de datos se refiere a la modificación de información personal para que los individuos no puedan ser identificados directamente. Esta técnica es esencial para proteger la privacidad en el tratamiento de grandes volúmenes de datos, como en la investigación y el análisis de datos. A través de métodos como la agregación, la perturbación de datos y la

Recepción: 07-06-2024 / Revisión: 10-07-2024 / Aprobación: 15-08-2024 / Publicación: 27-08-2024

generalización, se puede lograr la anonimización, permitiendo el uso de datos para diversos fines sin comprometer la identidad de los individuos.

Si bien la anonimización es beneficiosa para la protección de la privacidad, también plantea desafíos. Uno de los principales problemas es que la anonimización no siempre es irreversible. Técnicas avanzadas de reidentificación pueden combinar datos anonimizados con otras fuentes de información para revelar identidades individuales. Un estudio de la Universidad de Harvard, en 2020, reveló que hasta un 87% de las personas en un conjunto de datos anonimizados podían ser reidentificadas mediante técnicas de correlación de datos. Esto plantea un riesgo significativo para la privacidad y puede socavar la confianza en los procesos de anonimización. Además, la legislación sobre protección de datos, como el GDPR en la Unión Europea, establece estrictos requisitos para la anonimización de datos, y el incumplimiento puede resultar en sanciones severas para las organizaciones.

En Ecuador, el Código Orgánico Integral Penal (COIP) y la Ley de Protección de Datos Personales exigen que cualquier tratamiento de datos personales, incluyendo la anonimización, cumpla con los principios de legalidad, finalidad, proporcionalidad y transparencia. Las organizaciones deben asegurarse de que los datos anonimizados no puedan ser reidentificados y que se implementen medidas de seguridad adecuadas para proteger los datos durante todo el proceso de anonimización. La falta de cumplimiento puede llevar a sanciones administrativas y penales, lo que subraya la importancia de seguir las mejores prácticas y normativas en la gestión de datos personales.

Blockchain y su impacto en la privacidad

El Blockchain, una tecnología de registro distribuido, ha ganado popularidad por su capacidad para proporcionar transacciones seguras, transparentes y descentralizadas. Sin embargo, esta tecnología también plantea desafíos significativos en términos de privacidad y regulación.

Uno de los principios fundamentales del Blockchain es la transparencia, ya que todas las transacciones se registran en un libro mayor público que puede ser verificado por cualquier usuario de la red. Sin embargo, esta transparencia puede entrar en conflicto con las leyes de

Sinergia Académica ISSN: 2765-8252

Volumen: 7.
Nro. Especial 5
Año: 2024

Recepción: 07-06-2024 / Revisión: 10-07-2024 / Aprobación: 15-08-2024 / Publicación: 27-08-2024

protección de datos personales, como el derecho al olvido consagrado en el GDPR y otros marcos normativos. Las transacciones en Blockchain, una vez registradas, son prácticamente inmutables, lo que dificulta la eliminación de datos personales a petición de los individuos. Esta característica de inmutabilidad puede resultar en un conflicto directo con los derechos de privacidad y protección de datos.

Asimismo, las criptomonedas basadas en Blockchain, como Bitcoin, permiten realizar transacciones financieras de manera descentralizada y, en muchos casos, anónima. Esta característica puede ser explotada por ciberdelincuentes para lavar dinero, financiar actividades ilícitas y evadir impuestos, complicando la labor de las autoridades fiscales y las agencias de seguridad. La dificultad para rastrear las transacciones de criptomonedas y vincularlas a personas específicas presenta un desafío considerable para la lucha contra la ciberdelincuencia. A pesar de los esfuerzos para regular y monitorear el uso de criptomonedas, el anonimato y la descentralización que ofrecen continúan siendo atractivos para actividades ilícitas.

Planteamiento del problema

Incremento de los delitos cibernéticos

El panorama de la ciberdelincuencia ha experimentado un notable incremento en los últimos años, impulsado por la digitalización acelerada de diversas actividades económicas, sociales y personales. Este fenómeno ha expuesto tanto a individuos como a organizaciones a un mayor riesgo de sufrir ataques cibernéticos, evidenciando la necesidad de reforzar las estrategias de ciberseguridad y actualizar el marco jurídico para combatir eficazmente estos delitos.

Tabla 2. Pérdidas económicas causadas por delitos cibernéticos

Año	Pérdidas económicas globales (en billones de dólares)	Aumento anual (%)	Tipos de delitos más comunes
2019	1.5	20%	phishing, ransomware, fraude financiero

Recepción: 07-06-2024 / Revisión: 10-07-2024 / Aprobación: 15-08-2024 / Publicación: 27-08-2024

2020	3.0	100%	ransomware, malware, ataques de ingeniería social
2021	6.0	100%	ransomware, ataques a la cadena de suministro, phishing
2022	8.4	40%	ransomware, fraudes de criptomonedas, suplantación de identidad
2023	10.5	25%	ransomware, phishing, ataques a infraestructuras críticas
2024	12.0 (estimado)	14%	ransomware, malware, phishing

En Ecuador, las cifras también reflejan una tendencia preocupante. De acuerdo con el reporte de la Asociación Ecuatoriana de Ciberseguridad (AEC), el número de incidentes cibernéticos reportados en 2021 aumentó en un 45% en comparación con el año anterior. Entre los ataques más comunes se encuentran el phishing, el ransomware y el fraude financiero, afectando tanto a instituciones públicas como a empresas privadas y ciudadanos.

En 2022, Ecuador experimentó un incremento del 30% en ataques de ransomware, afectando notablemente a instituciones gubernamentales y empresas del sector privado. Además, los fraudes relacionados con criptomonedas también mostraron un incremento del 25%, impulsado por la creciente adopción de activos digitales en el país. Para 2023, los ataques dirigidos a infraestructuras críticas, como los sistemas de salud y transporte, incrementaron en un 35%, subrayando la necesidad de estrategias de ciberseguridad robustas.

El caso Ola Bini: un análisis de la ciberdelincuencia y la protección de datos en ecuador

Un ejemplo claro de las tensiones entre la seguridad informática y los derechos humanos es el caso de Ola Bini, un desarrollador de software sueco y defensor de la privacidad digital. Bini fue arrestado en Ecuador el 11 de abril de 2019, acusado de presunta participación en actividades de hacking y acceso no autorizado a sistemas informáticos del gobierno. La detención se produjo poco después de la revocación del asilo político de Julian Assange, fundador de WikiLeaks, en la

Sinergia Académica
ISSN: 2765-8252

Volumen: 7.
Nro. Especial 5
Año: 2024

Recepción: 07-06-2024 / Revisión: 10-07-2024 / Aprobación: 15-08-2024 / Publicación: 27-08-2024

embajada ecuatoriana en Londres, lo que llevó a especulaciones sobre posibles motivaciones políticas detrás del arresto de Bini.

Desde el principio, el caso de Ola Bini ha sido objeto de críticas por parte de defensores de derechos humanos y organizaciones internacionales que argumentan que las acusaciones carecen de pruebas concretas. Durante el proceso judicial, la defensa de Bini alegó que no había evidencia técnica que respaldara las afirmaciones de las autoridades y que se habían violado sus derechos fundamentales, incluyendo el debido proceso y la presunción de inocencia. A pesar de esto, Bini pasó más de dos meses en prisión preventiva antes de ser liberado bajo fianza, y su caso sigue pendiente de resolución.

El arresto de Ola Bini y las acusaciones en su contra generaron controversia, especialmente por la falta de claridad en las pruebas presentadas y las denuncias de violaciones a sus derechos procesales. Esto llevó a la presentación de la Causa No. 72-21-JD de Habeas Data en respuesta a la supuesta violación de los derechos de Bini a la protección de sus datos personales. Este recurso constitucional buscaba la transparencia y la corrección de los datos almacenados sobre Bini en las bases de datos del Estado ecuatoriano, alegando que la información recolectada y utilizada en su contra era incorrecta, desactualizada o había sido manipulada sin su consentimiento.

El Tribunal Constitucional, al analizar esta causa, debía determinar si se habían violado los derechos de Bini, conforme al artículo 92 de la Constitución. Un fallo favorable implicaría la obligación del Estado de rectificar y proteger adecuadamente los datos personales de Bini, además de establecer un precedente importante sobre la gestión de la información personal en casos de ciberdelincuencia.

El Código Orgánico Integral Penal (COIP) de Ecuador, específicamente en sus artículos 232 a 234, establece disposiciones para sancionar delitos informáticos, incluyendo el acceso no autorizado a sistemas informáticos, sabotaje cibernético y fraude electrónico. En el caso de Bini, las acusaciones se centraron en la violación de estos artículos, aunque la falta de pruebas contundentes ha generado controversia sobre la aplicación y eficacia de estas normativas.

Sinergia Académica
ISSN: 2765-8252

Volumen: 7.
Nro. Especial 5
Año: 2024

Recepción: 07-06-2024 / Revisión: 10-07-2024 / Aprobación: 15-08-2024 / Publicación: 27-08-2024

Impacto de la inteligencia artificial y el Big Data en la privacidad

La expansión de la inteligencia artificial (IA) y el análisis de grandes volúmenes de datos (Big Data) ha transformado la manera en que se gestionan y utilizan los datos personales, planteando serios desafíos para la privacidad individual. En este contexto, surge la preocupación por la capacidad de las empresas y entidades públicas para recopilar, almacenar y analizar grandes cantidades de información personal sin un adecuado consentimiento informado. La aplicación de algoritmos de IA para la toma de decisiones automatizadas, como en el ámbito del crédito o el empleo, introduce riesgos de discriminación y falta de transparencia, afectando directamente los derechos fundamentales de privacidad consagrados en la Constitución y las leyes de protección de datos. La necesidad de equilibrar la innovación tecnológica con la protección de la privacidad se convierte así en un imperativo jurídico y ético, requerido para asegurar que el desarrollo de la inteligencia artificial no comprometa los derechos individuales.

Las redes sociales han emergido como plataformas globales de interacción social y comercial, facilitando la comunicación instantánea y el intercambio de información personal entre millones de usuarios. Sin embargo, este fenómeno plantea desafíos en términos de protección de datos y privacidad. La recopilación masiva de datos por parte de estas plataformas, combinada con prácticas de monetización y publicidad dirigida, ha generado preocupaciones sobre la gestión ética y legal de la información personal. La regulación efectiva de las redes sociales implica establecer estándares claros en cuanto a la recopilación, uso y almacenamiento de datos personales, asegurando el respeto a los derechos individuales de privacidad y ofreciendo mecanismos efectivos para que los usuarios controlen la divulgación de su información. Este enfoque no solo protege la privacidad de los usuarios, sino que también promueve la confianza en las plataformas digitales como actores responsables en el manejo de datos sensibles.

Ciberseguridad en el sector financiero

El sector financiero enfrenta riesgos cibernéticos crecientes debido a la digitalización de servicios bancarios y financieros. La sofisticación de los ataques informáticos, como el phishing y el malware financiero, pone en riesgo la seguridad de la información personal y financiera de los

Sinergia Académica
ISSN: 2765-8252

Volumen: 7.
Nro. Especial 5
Año: 2024

Recepción: 07-06-2024 / Revisión: 10-07-2024 / Aprobación: 15-08-2024 / Publicación: 27-08-2024

clientes. En respuesta, las instituciones financieras deben implementar medidas robustas de ciberseguridad que cumplan con normativas nacionales e internacionales, como las directrices de la Autoridad de Control y Supervisión Financiera. Estas medidas incluyen la adopción de sistemas avanzados de detección de intrusos, la encriptación de datos sensibles y la educación continua del personal en prácticas seguras de tecnología de la información. La protección efectiva de los datos financieros no solo protege los intereses económicos de los clientes, sino que también fortalece la estabilidad del sistema financiero en su conjunto, promoviendo la confianza del público y mitigando riesgos sistémicos.

La expansión del entorno digital plantea importantes interrogantes sobre cómo proteger adecuadamente los derechos digitales y las libertades civiles en un contexto de creciente vigilancia y control tecnológico. El derecho a la privacidad, consagrado en la Constitución y en tratados internacionales, debe adaptarse a las realidades de la era digital, donde la recopilación y análisis masivo de datos pueden comprometer la intimidad y la autonomía de los individuos. La regulación de la vigilancia digital y el uso de tecnologías de reconocimiento facial, por ejemplo, requiere un equilibrio entre la protección de la seguridad pública y el respeto a los derechos individuales. El desarrollo de políticas públicas que salvaguarden la privacidad digital, como el derecho al olvido en internet y la protección de datos biométricos, es crucial para preservar la libertad de expresión y la autodeterminación personal en la era digital.

Discusión

El aumento de la ciberdelincuencia en Ecuador, que incluye delitos como el phishing, ransomware, y robo de identidad, evidencia la necesidad urgente de fortalecer las leyes y estrategias de ciberseguridad. Aunque la legislación ecuatoriana ha avanzado en la protección de datos y la tipificación de delitos informáticos, enfrenta retos debido a la rápida evolución tecnológica y las tácticas de los delincuentes. Las tecnologías emergentes como la criptografía, la anonimización de datos y el Blockchain complican la regulación actual, exigiendo un marco normativo flexible y actualizado. Además, la cooperación internacional es esencial para enfrentar estos delitos transnacionales, siendo vital la armonización de legislaciones y el intercambio de

Sinergia Académica ISSN: 2765-8252

Volumen: 7.
Nro. Especial 5
Año: 2024

Recepción: 07-06-2024 / Revisión: 10-07-2024 / Aprobación: 15-08-2024 / Publicación: 27-08-2024

información, con iniciativas como el Convenio de Budapest proporcionando un marco para la colaboración efectiva.

Conclusión

La ciberdelincuencia y la protección de datos personales representan desafíos cada vez más urgentes en la sociedad digital contemporánea. El incremento de los delitos cibernéticos y la vulnerabilidad de los datos personales demandan respuestas efectivas tanto a nivel legislativo como tecnológico. Es imperativo que los sistemas jurídicos adapten y fortalezcan sus marcos normativos para garantizar la seguridad y privacidad de los individuos en el espacio digital.

La regulación adecuada de la ciberseguridad y la protección de datos no solo es una cuestión de cumplimiento normativo, sino también de respeto a los derechos fundamentales de los ciudadanos. Los avances tecnológicos, si bien ofrecen beneficios significativos en términos de eficiencia y comunicación, también requieren que las autoridades y las empresas adopten medidas proactivas para mitigar los riesgos asociados con la manipulación indebida de información personal y financiera.

Por lo tanto, se hace necesario fomentar una cultura de ciberseguridad desde la educación primaria hasta el ámbito empresarial, promoviendo la concienciación sobre buenas prácticas en el uso de tecnologías digitales. Esto, junto con la colaboración internacional y el desarrollo continuo de tecnologías de protección, permitirá construir un entorno digital más seguro y confiable para todos los usuarios. Solo mediante un enfoque integral y colaborativo podremos enfrentar los retos emergentes en la ciberseguridad y proteger efectivamente los derechos de privacidad en la era digital.

Referencias

Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL). (2022). *Agencia de Regulación y Control de las Telecomunicaciones* (ARCOTEL). https://www.arcotel.gob.ec/incidentes-datos-sistemas-2022

Recepción: 07-06-2024 / Revisión: 10-07-2024 / Aprobación: 15-08-2024 / Publicación: 27-08-2024

Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL). (2022). *Informe de seguridad digital en Ecuador*. https://www.arcotel.gob.ec/informe-seguridad-digital-2022

Centro de Respuesta a Incidentes Informáticos del Ecuador (ECU-CERT). (2022). *Informe de ataques DDoS*. https://www.ecu-cert.gob.ec/informe-ddos-2022

Centro de Respuesta a Incidentes Informáticos del Ecuador (ECU-CERT). (2022). *Reporte anual de incidentes cibernéticos.* https://www.ecu-cert.gob.ec/reporte-anual-2022

Codigo Organico Integral Penal (COIP). (2014). *Delitos contra la seguridad de los activos de los sistemas de información y comunicación* (Sección Tercera). *Lexis*, 297. https://www.defensa.gob.ec/wp-content/uploads/downloads/2021/03/COIP_act_feb-2021.pdf

Colón, E., & Cuenca, H. (2014). Cómo responder a un Delito Informático. *Redalyc*, *7*(11), 43-50. https://www.redalyc.org/pdf/5826/582663858004.pdf

Constitución de la República del Ecuador. (2008). *Acción de Hábeas Data* (Sección Quinta). *Lexis*, 136. https://www.oas.org/juridico/pdfs/mesicic4_ecu_const.pdf

Enríquez, L. (2021). *Caso Ola Bini: la presunción de inocencia en entornos digitales y el derecho al cifrado.* Universidad Andina Simon Bolivar. https://www.uasb.edu.ec/ciberderechos/2021/06/15/caso-ola-bini-la-presuncion-de-inocencia-en-entornos-digitales-y-el-derecho-al-cifrado/

Fiscalía General del Estado. (2021). *Delitos informáticos en Ecuador.* https://www.fiscalia.gob.ec/delitos-informáticos-ecuador-2021

Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL). (2022). R*eporte de intercepción ilícita de comunicaciones.* https://www.mintel.gob.ec/reporte-intercepción-ilícita-2022

Ministerio del Interior. (2022). *Estadísticas de acceso ilícito a sistemas informáticos*. https://www.ministeriodelinterior.gob.ec/estadísticas-delitos-informáticos-2022

Volumen: 7.
Nro. Especial 5
Año: 2024

Recepción: 07-06-2024 / Revisión: 10-07-2024 / Aprobación: 15-08-2024 / Publicación: 27-08-2024

Narvaez, D. (2015). El delito informático y su clasificación. *Redalyc, 2*(2), 158-173. https://www.redalyc.org/pdf/5646/564660011007.pdf

Neif, S., & Espina, J. (2006). Ética Informática en la Sociedad de la Información. *Scielo, 11*(36). https://ve.scielo.org/scielo.php?script=sci_arttext&pid=S1315-99842006000400004

Policía Nacional de Ecuador. (2021). *Informe sobre delitos cibernéticos en Ecuador*. https://www.policiaecuador.gob.ec/informe-delitos-cibernéticos-2021

Pons Gamón, V. (2017). Internet, la nueva era del delito: ciberdelito,ciberterrorismo,legislación y ciberseguridad. *Scielo*(20). http://scielo.senescyt.gob.ec/pdf/urvio/n20/1390-4299-urvio-20-00080.pdf

Pullaguari, K. (2019). Politización mediática de la justicia en Ecuador. Estudio de caso: Ecuavisa. *Redalyc, 9*(2), 17. doi:https://doi.org/10.15517/h.v9i2.37659

Saltos, M., Robalino, J., & Pazmiño, L. (2021). Análisis conceptual del delito informático en Ecuador. *Scielo, 17*(78), 343-351. http://scielo.sld.cu/pdf/rc/v17n78/1990-8644-rc-17-78-343.pdf

Sancho, C. (2017). Ciberseguridad. Presentación del dossier. *Scielo*(20), 8-15. http://dx.doi.org/10.17141/urvio.20.2017.2859

Superintendencia de Telecomunicaciones. (2022). *Denuncias por intercepción ilegal de comunicaciones*. https://www.supertel.gob.ec/denuncias-intercepción-2022

Vargas, R. (2017). Ciberdefensa y ciberseguridad, más allá del mundo virtual. *Redalyc*(20), 31-45. https://doi.org/10.17141/urvio.20.2017.2571