Análisis sobre la integración de la inteligencia artificial en la lucha contra la ciberdelincuencia en el Ecuador: desafíos y perspectivas

Analysis on the integration of artificial intelligence in the fight against cybercrime in Ecuador: Challenges and perspectives

Análise sobre a Integração da Inteligência Artificial no Combate ao Cibercrime no Equador: Desafios e Perspectivas

• Fecha de recepción: 2024/04/17
• Fecha de evaluación: 2024/08/07
• Fecha de aprobación: 2024/08/14

Para citar este artículo / To reference this article / Para citar este artigo: Maldonado-Montenegro, Ch. (2024). Análisis sobre la integración de la inteligencia artificial en la lucha contra la ciberdelincuencia en el Ecuador: desafíos y perspectivas. *Revista Criminalidad, 66*(3), 27-44. https://doi.org/10.47741/17943108.660

Christian Daniel Maldonado Montenegro
Magíster en Gestión de Riesgos
Policía Nacional del Ecuador
Quito, Ecuador
maldo2001@hotmail.com
https://orcid.org/0000-0003-0519-0301

Resumen

En el Ecuador, la creciente adopción de tecnologías digitales ha traído consigo tanto beneficios como desafíos. En este último, destaca la proliferación de ciberdelincuentes en el país. En este escenario, el presente estudio analiza la integración de la inteligencia artificial (IA) en la lucha contra la ciberdelincuencia. Para ello, se empleó una metodología que combinó la investigación documental con el uso de encuestas a expertos en ciberseguridad pertenecientes a la Unidad Nacional de Ciberdelito de la Policía Nacional del Ecuador. Este enfoque permitió obtener información detallada del estado actual del cibercrimen en el país y las posibles soluciones que involucran a la IA. Los resultados obtenidos revelaron la existencia de vulnerabilidades significativas en diversos sectores de la sociedad, tanto para empresas privadas como públicas. Además, se identificaron como ciberdelitos comunes el robo de información sensible, el phishing y la suplantación de identidad. Por consiguiente, se comprobó que la IA puede ser un complemento valioso en este contexto. Si se integra a los procesos actuales, puede brindar una protección más efectiva a los sistemas y base de datos, tanto para la prevención como para la solución a diversos ciberataques.

Palabras clave:

Detección de delitos; inteligencia artificial; internet; ciberdelincuencia; ciberseguridad

Abstract

In Ecuador, the growing adoption of digital technologies has brought with it both benefits and challenges. Among the latter, the proliferation of cybercriminals in the country stands out. In this scenario, this study analyses the integration of artificial intelligence (AI) in the fight against cybercrime. For this purpose, a methodology was employed that combined documentary research with the use of surveys of cybersecurity experts belonging to the National Cybercrime Unit of the National Cybercrime Unit of the National Police of Ecuador. This approach made it possible to obtain detailed information on the current state of cybercrime in the country and possible solutions involving AI. The results obtained revealed the existence of significant vulnerabilities in various sectors of society, both for private and public companies. In addition, the theft of sensitive information, phishing

and identity theft were identified as common cybercrimes. Consequently, it was found that AI can be a valuable complement in this context. If integrated into current processes, it can provide more effective protection to systems and databases for both prevention and remediation of various cyber-attacks.

Keywords:

Crime detection; artificial intelligence; internet; cybercrime; cybersecurity

Resumo

No Equador, a crescente adoção de tecnologias digitais trouxe benefícios e desafios. Quanto a estes últimos, destaca-se a proliferação de criminosos cibernéticos no país. Nesse cenário, neste estudo, analisa-se a integração da inteligência artificial (IA) na luta contra o crime cibernético. Para isso, empregou-se uma metodologia que combinou pesquisa documental com o uso de pesquisas com especialistas em segurança cibernética pertencentes à Unidade Nacional de Crimes Cibernéticos da Polícia Nacional do Equador. Essa abordagem nos permitiu obter informações detalhadas sobre a situação atual do crime cibernético no país e possíveis soluções que envolvem a IA. Os resultados obtidos revelaram a existência de vulnerabilidades significativas em vários setores da sociedade, tanto para empresas privadas quanto públicas. Além disso, o roubo de informações confidenciais, o phishing e o roubo de identidade foram identificados como crimes cibernéticos comuns. Consequentemente, descobriu-se que a IA pode ser um complemento valioso nesse contexto. Se integrada aos processos atuais, ela pode proporcionar uma proteção mais eficaz de sistemas e bancos de dados, tanto para a prevenção quanto para a correção de vários ataques cibernéticos.

Palavras chave:

Detecção de crimes; inteligência artificial; internet; crime cibernético; segurança cibernética

Introducción

En el Ecuador, la tecnología ha avanzado a un ritmo acelerado, permitiendo una alta circulación de información, personas y bienes. Es decir, asistimos a una verdadera transformación en todos los sentidos. El internet se ha popularizado y se ha convertido en un instrumento de comunicación y transmisión de información, así como de interacción entre personas para las más diversas actividades, en todos los rincones del país. Esta conexión global se ha convertido en un relevante facilitador para importantes sectores sociales como la educación, la ciencia, los negocios; y, como lo demuestran las últimas elecciones, el sector político también desempeña un papel fundamental. Sin embargo, a pesar de los grandes beneficios que ha traído internet, también ha traído consigo algunos problemas, uno de los cuales es el ciberdelito.

Es decir, la población pasó a vivir no solo con los beneficios derivados de esta innovación, sino también con sus perjuicios, puesto que el internet posibilita que el ciberdelito no tenga límites territoriales, como otros delitos transnacionales, con la agravante de que el delincuente no necesita desplazarse para realizar la inconducta. En definitiva, una persona puede practicar innumerables conductas nocivas sin salir de su hogar.

Esta situación ha impactado al Ecuador de manera significativa. Con el paso de los años, se ha observado un marcado aumento en las cifras de ciberdelincuentes en el país. Por ejemplo, en el 2016 se registraron 8796 casos de ciberdelitos y esta tendencia al alza se ha mantenido hasta el 2019, donde se reportaron 10 279 denuncias por delitos virtuales (DNTIC, 2020). Complementando estas estadísticas, el diagnóstico de ciberseguridad publicado por el Ministerio de Telecomunicaciones y la Sociedad de la Información revela un incremento exponencial del 100 % en los delitos cometidos a través de medios electrónicos para el 2020 (MINTEL, 2022).

El informe también destaca que, según el sistema centralizado norteamericano *Cyber Tipline*, se contabilizaron

242631 incidentes relacionados con la explotación infantil en línea durante ese mismo año. Al mismo tiempo, se registraron 896 denuncias por apropiación fraudulenta, 212 denuncias por estafa y 66 denuncias por delitos de pornografía infantil. Es importante destacar que, lamentablemente, los adultos mayores, los niños y adolescentes son los principales blancos de estos actos delictivos (MINTEL, 2022).

El análisis de la situación actual revela una falta de políticas específicas para abordar eficazmente este fenómeno (Juca y Medina, 2023). La ausencia de herramientas tecnológicas sofisticadas para la detección y prevención de delitos en entornos digitales, así como la falta de actualización en los sistemas de procesamiento de información, dificulta el cumplimiento efectivo de la protección ciudadana y la resolución de casos relacionados con la ciberdelincuencia (FGE, 2021).

En este contexto, este artículo se propone examinar el impacto potencial de la integración de la inteligencia artificial en el combate contra los delitos cibernéticos en Ecuador. Se llevó a cabo una evaluación exhaustiva del estado actual de la ciberdelincuencia en el país, identificando los tipos más prevalentes de delitos y los sectores más vulnerables. Asimismo, se analizaron las tecnologías basadas en la inteligencia artificial que pueden aplicarse específicamente en estas áreas.

Para alcanzar estos objetivos, se partió de un análisis detallado de estudios previos sobre ciberdelitos, su contexto y características principales. Posteriormente, se realizaron entrevistas a cinco especialistas en ciberseguridad de la Policía Nacional del Ecuador, las cuales servirán de base para identificar cómo la inteligencia artificial puede integrarse a los procesos de prevención contra la ciberdelincuencia en el país.

Desarrollo teórico

Evaluación del estado actual de la ciberdelincuencia en Ecuador

Ciberdelincuencia en el Ecuador

En la era digital contemporánea, la ciberdelincuencia ha emergido como una amenaza omnipresente, afectando a individuos, empresas y gobiernos en todo el mundo. En particular, Ecuador no ha sido inmune a esta creciente problemática, enfrentándose a una serie de desafíos en la protección de sus sistemas digitales y la salvaguarda de la información sensible. Según el informe de amenazas en tiempo real de *Kaspersky Lab*, en el 2017, Ecuador ocupó el primer lugar de América del Sur y el quinto a nivel mundial, con 2.8 % de ciberataques a sus redes (Freire, 2017). De estos, el 49.05 % estaban asociados a servidores de RDP (Protocolo de Escritorio Remoto) a través de invasiones de "fuerza bruta" (*bruteforce generic* RDP): este método de ataque implica explorar rangos de direcciones de IP y puertos TCP para simular ser clientes autorizados del servicio, y una vez encontrado un servidor RDP vulnerable toma el control total de los recursos almacenados (Freire, 2017).

Es importante resaltar que, en Ecuador, el 43 % de la población tiene acceso a internet; no obstante, no existe una cultura de protección de datos o prevención de amenazas. Esta carencia sobre el tema informático hace que sean fácilmente víctimas de los ciberataques (Loor et al., 2023). Sin embargo, esta realidad no solo la vive la parte civil del país; existen grandes ataques cibernéticos a instituciones públicas y privadas, como se describen a continuación.

En primer lugar, el caso de la Corporación Nacional de Telecomunicaciones (CNT), perpetrado el 16 de julio de 2021, donde la entidad fue víctima de un ciberataque que la mantuvo 15 días sin procesos administrativos y de facturación. Esta agresión a su sistema fue denunciada ante la Fiscalía y comunicada en su página web oficial, donde se expuso que fue víctima de un virus *Ransomware EXX* (Dávalos, 2021), lo que provocó la alteración de las áreas de facturación, activaciones de planes y recargas. Este hecho indica que, a pesar de que su data center es de nivel TIER III, lamentablemente con tecnología especializada, los ataques cibernéticos la vuelven vulnerable (Acaro, 2023).

Seguido a este ataque, en el mismo año, el Banco del Pichincha sufrió dos ciberataques, uno en febrero a manos de un hacker actor llamado *Hotarus Corp*, que involucró al Ministerio de Finanzas, lo que provocó la pérdida de 80 gigabytes de información secuestrada de la entidad gubernamental y del banco en un tiempo de 13 días (Seguridad 360, 2021). El segundo ataque tuvo lugar el 11 de octubre. Este trajo consecuencias más significativas: el banco se vio obligado a suspender sus operaciones, lo que dejó sin funcionamiento a miles de servicios automáticos y al portal de banca *online*. Este incidente fue considerado internacionalmente como uno de los mayores ataques de ese año (Abrams, 2021).

En este segundo caso, una banda de *Ransomware* utilizó la herramienta *Pentesting Cobal Strike* (Harán, 2021). Este producto instala un agente llamado *Bacon*, mediante el cual se extraen comandos, el registro de claves, el *proxy SOCKS*, el escaneo de puertos, entre otros. Muchas veces estos software llegan al sistema mediante correos electrónicos infectados con anuncios maliciosos (CSIRT - EPN, 2021).

Igualmente, otra entidad pública afectada fue la Agencia Nacional de Tránsito (ANT, 2021), la cual sufrió un ataque a su sistema *AXIS*. Este ciberataque duró 48 horas. No obstante, las repercusiones se extendieron por al menos tres meses. Como resultado, 110 000 procesos de matriculación se realizaron de manera fraudulenta y 50 000 procesos regulatorios terminaron anulados (Rosero, 2021).

Según Montes y Vergara (2023), los ataques cibernéticos a diferentes entidades privadas o públicas eran cuestión de tiempo, ya que en su investigación evidenciaron que desde el 2014 al 2022, en cada año se presentaron diversos tipos de ataques, tanto por *hardware* o *malware*. En el 2014, se registraron 38 % de ataques por *malware*, mientras que para el 2022 se observa un aumento del 60 %, lo que indica que los ataques se intensifican debido a la acción de hackers con mayor experiencia y con acceso a medios tecnológicos avanzados. Esta tendencia al alza en los ataques cibernéticos resalta la importancia de tomar medidas preventivas para proteger la información y los sistemas.

Durante el 2022, el 10 de marzo, la plataforma del Centro de Inteligencia Estratégica (CIES) sufrió un ataque que comprometió toda la información procesada por la institución, incluyendo los subsistemas de inteligencia de la Policía y las Fuerzas Armadas. El 16 de abril, el municipio del Distrito Metropolitano de Quito también fue víctima de un ciberataque. En este caso, un *malware* tipo *Ransomware* de la cepa *Black Cat*, afectó el 20 % de la base de datos municipal; en este caso, el ataque pudo ser detenido a tiempo (Onofa, 2022).

Con base en estos datos, se observa un incremento constante de la frecuencia y la complejidad de los ataques cibernéticos en el país. Esto pone de manifiesto una necesidad urgente de implementar medidas más sólidas de seguridad cibernética, a nivel individual e institucional. Es esencial brindar una respuesta integral y coordinada que aborde tanto las vulnerabilidades técnicas como las deficiencias en la conciencia y la preparación frente a estas amenazas. Para lograrlo, se deben fomentar campañas de sensibilización sobre los riesgos cibernéticos, fortalecer la capacitación del personal en materia de seguridad informática e invertir en tecnologías de protección de datos más robustas.

Tipos prevalentes de ciberdelincuencia

Tipos de ciberdelitos

Según la revista *Forbes Ecuador* (2023), los tipos de ciberdelitos más comunes en el país son:

1. Instalación de virus: estos virus se instalan en los dispositivos de las víctimas para recopilar contraseñas, datos personales, información financiera e incluso los registros de navegación. Los datos son posteriormente utilizados para fines ilícitos, como el fraude de identidad, el robo de dinero o envíos de correos spam.
2. Robo de datos confidenciales y bancarios: los ciberdelincuentes utilizan técnicas como el *phishing* y el *malware* para acceder a ordenadores o teléfonos móviles de terceros para robar información confidencial, como números de tarjetas de crédito y contraseñas. Esta información puede ser utilizada para realizar compras fraudulentas, robar dinero de cuentas bancarias o incluso suplantar la identidad de la víctima.
3. Falsificación de documentos: los ciberdelincuentes utilizan los datos robados para falsificar documentos, como pasaportes, licencias de conducir y estados financieros. Estos documentos falsificados pueden ser utilizados para cometer diversos delitos, como el fraude y robo de identidad y la evasión de impuestos.
4. Extorsión: al robar la información, los ciberdelincuentes utilizan fotos, videos privados o mensajes de texto, para luego amenazar con divulgarlos si no se paga un rescate. Este tipo de ciberdelito puede tener un impacto psicológico devastador en las personas afectadas.

La revista recalca que tanto los civiles como las entidades deben tomar medidas para protegerse del cibercrimen, como instalar software antivirus y evitar compartir información personal en línea.

Según datos de Kaspersky (2024), portal que monitorea información sobre ciberataques, los principales tipos de ciberdelincuencia en el mundo son los delitos de intrusión (71 millones de casos) y el *malware* (18 millones de casos). El portal de datos expone que existen diferentes tipos de ciberdelincuentes:

- Altamente calificados: son los hackers que poseen profundo conocimiento en informática y utilizan herramientas sofisticadas y complejas para realizar ciberataques. Suelen ser difíciles de rastrear debido a su alto nivel de experiencia y a las técnicas avanzadas que emplean.
- Principiantes: son los que utilizan métodos más simples y menos elaborados. Sus principales técnicas son el *phishing* o *malware* básico enviado por redes sociales o correos electrónicos. Suelen ser más fáciles de rastrear y capturar por las autoridades.

Los delitos más comunes en Ecuador

Tabla 1. | Tipos de delitos cibernéticos en el Ecuador

Artículo	Tipo penal
103	Pornografía con utilización de niñas, niños o adolescentes
104	Comercialización de pornografía con utilización de niñas, niños o adolescentes
154.1	Instigación al suicidio
154.2	Hostigamiento
166 inc. 2	Acoso sexual (inciso 2 - Ciberacoso sexual)
168	Distribución de material pornográfico a niñas, niños y adolescentes
173	Contacto con finalidad sexual con menores de dieciocho años por medios electrónicos
174	Oferta de servicios sexuales con menores de dieciocho años por medios electrónicos.
178	Violación a la intimidad
185	Extorsión
186 ns. 1 y 2	Estafa (numerales 1 y 2 por medio electrónico)
190	Apropiación fraudulenta por medios electrónicos
191	Reprogramación o modificación de información de equipos terminales móviles
193	Reemplazo de identificación de terminales móviles
194	Comercialización ilícita de terminales móviles
195	Infraestructura ilícita
208B	Actos lesivos a los derechos de autor
212	Suplantación de identidad
323	Captación ilegal de dinero
366 n. 1	Terrorismo (numeral 1)

Nota: La tabla expone los tipos de delitos según la Ley Orgánica de Protección de Datos.

Fuente: Gobierno Electrónico de Ecuador (2019).

La tabla 1 muestra los tipos de delitos cometidos por hackers que se apropian y descargan de forma fraudulenta la información obtenida en internet para luego venderla al mejor postor (DNTIC, 2020). Este proceso se lleva a cabo por medio de vectores de ataque, que son rutas o medios que un atacante puede utilizar para obtener acceso no autorizado a una computadora o red, con el fin de ejecutar un comando destructivo o comprometer los datos de una empresa o de una persona (Gárate, 2023). Algunos vectores de ataque comunes son el *malware*, los virus, los archivos adjuntos de correo electrónico, las páginas web, las ventanas emergentes, la mensajería instantánea, los mensajes de texto y la ingeniería social (Tejedor, 2023).

Además, en general, se pueden dividir los ataques en dos grupos: pasivos y activos.

Pasivo: se produce cuando el ataque intenta obtener acceso o utilizar información del sistema sin afectar los recursos de este. Por ejemplo: *typosquatting, phishing* y otros ataques basados en ingeniería social (Tejedor, 2023).

Activo: ocurre cuando el ciberdelincuente intenta cambiar un sistema o afectar su funcionamiento, explotando vulnerabilidades no parcheadas, falsificando correos electrónicos o recurriendo a *Man in the Middle* (MitM), secuestro de dominio y *Ransomware* (Tejedor, 2023).

Dicho esto, la mayoría de los vectores de ataque comparten algunas similitudes y siguen una ruta lógica usual:

- El hacker identifica un objetivo potencial.
- El pirata informático recopila información sobre el objetivo mediante ingeniería social, *malware, phishing*, OPSEC (operaciones de seguridad) y escaneo automatizado de vulnerabilidades.
- Luego, el atacante utiliza esta información para identificar posibles vectores de ataque y crear o equiparse con herramientas para explotarlos.
- El atacante obtiene acceso no autorizado al sistema y roba datos confidenciales o instala códigos maliciosos.

Así, el atacante monitorea la computadora o la red, roba información o utiliza recursos informáticos para extraer datos relevantes.

Principales ciberamenazas en el Ecuador

A continuación, se destacan los ataques de piratas informáticos más comunes.

DDOS Attack

Según Llangarí (2016), el principal objetivo de este ataque es sobrecargar las actividades del servidor informático específico, provocando que se ralentice y haciendo que los sitios web no estén disponibles para el acceso. Esto sucede a través de una red llamada *zombie* con computadoras que ya están infectadas y se conectan al maestro hacker. Al elegir el objetivo, esta red informática se encarga de sobrecargar el sistema con el objetivo de hacerlo inaccesible.

Este tipo de ataque se presentó en el medio digital, La Posta, donde su página web quedó totalmente inhabilitada por 48 horas. No se reportaron daños masivos al sistema; sin embargo, los investigadores determinaron que al menos 27 millones de ingresos a su sistema provinieron del extranjero (Fundamedios, 2024).

Ransomware

Para Coello (2021), el *Ransomware* es un *malware* capaz de bloquear la computadora y cifrar archivos. Con esto, el hacker toma el control del dispositivo y exige una recompensa en efectivo para activar nuevamente los servicios de la máquina. Con él, el hacker obtiene el control de todos los archivos e información de la víctima, además de tener el poder de controlarlos de forma remota, lo que puede dificultar que el usuario identifique el problema.

El *modus operandi* funciona a través de una estrategia llamada "ingeniería social", donde los delincuentes inducen a la víctima a acceder a enlaces de mensajes y anuncios convincentes, lo que resulta en la instalación de un virus camuflado. Este tipo de ciberataque es el más utilizado en el Ecuador, tanto para empresas públicas como privadas (Coello, 2021).

Phishing

Consiste en un ciberataque en el que los piratas informáticos engañan a los usuarios para que entreguen información confidencial, incluidas contraseñas, datos bancarios y CPF. Por lo general, este tipo de ciberdelito dirige al usuario a un sitio web idéntico; por ejemplo, a una sucursal bancaria real. En esta página falsa, que funciona como cebo, los piratas informáticos pescan datos de los usuarios (Suastegui, 2022).

El *phishing* es uno de los ciberataques más populares en la actualidad. Según Echeverría (2024), en el contexto actual de crisis de seguridad en el país, los ciberdelincuentes han encontrado un clima de miedo y urgencia perfecto para lanzar ataques de *phishing*. Utilizan mensajes maliciosos, correos electrónicos y mensajes con enlaces que parecen provenir de entidades o empresas legítimas. Tal es el caso de la red social X, donde se han detectado enlaces fraudulentos en noticias que informan sobre la seguridad en Ecuador. Estos enlaces, en realidad, contienen software malicioso (Echeverría, 2024).

Ataques de fuerza bruta (brute force attack)

Un ataque de fuerza bruta, como lo definen Bravo et al. (2021), consiste en el robo de contraseñas mediante la ejecución de numerosos intentos repetidos y automatizados de combinar nombre de usuario y contraseña. La principal razón por la que se llevan a cabo estos ataques es su facilidad de ejecución. Gracias a la automatización mediante *scripts*, es posible probar cientos o miles de servidores al mismo tiempo (Albors, 2020). Posteriormente, esta información puede ser utilizada para explotar anuncios o datos de usuarios para obtener ganancias financieras.

Legislación aplicable

Para abordar de manera efectiva el problema del ciberdelito, es fundamental comprender su origen, causas, motivaciones y diversos actores que participan. Este conocimiento permite desarrollar políticas y herramientas a nivel nacional, empresarial y personal.

En este sentido, con la implementación del Código Orgánico Integral Penal (COIP) en el 2014, Ecuador estableció un marco legal para abordar los desafíos y riesgos asociados al uso de internet. Ochoa (2021), en su investigación sobre los "Desafíos mundiales del cibercrimen", analizó la aplicación de los artículos del COIP en el país durante un periodo de cinco años. Su estudio reveló que, hasta el 2018, se habían presentado 1265 denuncias en la Fiscalía General del Estado relacionadas con ciberdelitos, de los cuales 1072 casos han sido resueltos, es decir, archivados, desestimados o dictaminados. No obstante, en el ámbito penal, el COIP ha incorporado quince disposiciones sobre delitos informáticos que abarcan conductas similares a los delitos tradicionales, descritos con anterioridad en la tabla 1.

Vulnerabilidad de los sectores privados y gubernamentales

Según la Fiscalía General del Estado (FGE, 2021), existen diversos parámetros que hacen vulnerables a las entidades gubernamentales y privadas a un ataque

cibernético. Estos parámetros se pueden agrupar en las siguientes categorías:

1. Déficit en la investigación digital: desconocimiento de las técnicas de investigación digital. Los agentes del orden público poseen un conocimiento parcial sobre cómo obtener, asegurar y presentar evidencia digital. La falta de regulación clara sobre las técnicas forenses admisibles en los tribunales genera que muchas de las evidencias en este ámbito sean desestimadas.
2. Falta de programas metodológicos: el informe de la Fiscalía General del Estado (FGE), señala que existen falencias en la planificación adecuada para la búsqueda, recolección y análisis de las pruebas digitales. Se hace necesario implementar aproximaciones interdisciplinarias y colaborativas para resolver estas deficiencias.
3. Carencia de recursos tecnológicos: falta de herramientas tecnológicas. La investigación digital requiere equipos y software especializados que, en muchos casos, no están disponibles debido a su alto costo. La inversión en software licenciado es fundamental para fortalecer la capacidad de investigación en este ámbito.
4. Vacíos en la normativa internacional: falta de armonización en la normativa internacional. Las diferentes legislaciones nacionales dificultan la investigación y persecución de cibercrímenes trasnacionales. Es necesario establecer mecanismos de cooperación internacional para armonizar las leyes y facilitar la lucha contra este tipo de delitos.

En conclusión, la lucha contra el cibercrimen enfrenta varios desafíos que requieren soluciones multifacéticas. Se necesitan medidas para mejorar el conocimiento y las habilidades de los investigadores, fortalecer la cooperación internacional y desarrollar herramientas metodológicas adecuadas.

En este contexto, el Centro de Respuesta a Incidentes de la Agencia de Regulación y Control de Telecomunicaciones (Arcotel) desempeña un papel primordial en la protección del ciberespacio ecuatoriano. La misión de esta entidad es brindar apoyo en la prevención y resolución de incidentes de seguridad informática, tanto para instituciones del sector público como privado. De esta manera, Arcotel contribuye a mejorar la seguridad de las redes de telecomunicaciones de todo el país y el uso seguro de la red. Se debe destacar que la entidad colabora estrechamente con otros equipos de respuesta a incidentes informáticos (CERT y CSIRT) dentro y fuera del Ecuador (EcuCERT, 2024).

Detección de los ciberdelitos

Las detecciones de intrusiones se llevan a cabo a través del Centro de Respuesta a Incidentes Informáticos EcuCERT, utilizando los siguientes métodos:

Red de confianza: los miembros de EcuCERT reportan los incidentes mediante informes que incluyen información como la dirección IP, la fecha, la hora y el puerto del sistema o aplicación afectada. Además, el programa puede configurar automáticamente el servidor para rechazar las conexiones desde la dirección IP atacante.

Programas de análisis de *logs*: estos programas buscan patrones que indiquen posibles ataques, como intentos de acceso por fuerza bruta. Las herramientas usadas son *Fail2ban*, una aplicación escrita en Python para la prevención de instrucciones, y la *IP-tables*, que es la herramienta que configura el firewall del sistema operativo Linux.

Esta comunidad es un proveedor de servicios conformado por la Agencia de Regulación y Control de las Telecomunicaciones. Para acceder a esta protección, las empresas privadas deben contratar sus servicios. En el caso de la ciudadanía, pueden realizar denuncias directamente a través del portal EcuCERT.com.

No obstante, también se puede enfatizar que el país ha establecido diferentes entidades gubernamentales en el ámbito de la lucha contra los ciberdelitos. Por ejemplo, el Ministerio de Defensa Nacional, que es rector de la ciberseguridad en el ámbito militar; el Ministerio de Telecomunicaciones y la Sociedad de la Información (MINTEL), que lidera la seguridad civil; la Política Nacional de Ciberseguridad (PNC), publicada en el 2021, la cual establece siete pilares para la protección del ciberespacio; y la Estrategia Nacional de Ciberseguridad en el Ecuador (ENCE), publicada en el 2022, que define seis ejes de acción para la gestión de la ciberseguridad. Sin embargo, a pesar de este avance en el marco regulatorio y estratégico, todavía quedan muchos desafíos que superar, como lo evidencian las estadísticas descritas en apartados anteriores.

Uso de la inteligencia artificial en la lucha contra la ciberdelincuencia

La inteligencia artificial (IA) desempeña varias funciones importantes en la lucha contra la delincuencia digital. Para Esquivel y Recalde (2023), la IA se puede entrenar para identificar patrones inusuales o actividades sospechosas en redes y sistemas informáticos. Esto incluye la detección de intentos de piratería, actividad de *malware* y comportamiento de usuario malicioso.

Dado que cada día se generan enormes cantidades de datos en internet, la inteligencia artificial se puede utilizar para analizar estos datos y extraer información valiosa de ellos. Esto implica identificar tendencias, patrones de comportamiento y correlaciones entre diferentes tipos de actividad criminal. Se utiliza para detectar y prevenir fraudes financieros como el robo de identidad, transacciones fraudulentas y esquemas de *phishing*. Los algoritmos de aprendizaje automático pueden analizar patrones de transacciones y comportamiento de los usuarios para identificar actividades sospechosas en tiempo real (CCN-CERT, 2023).

La Interpol (2024) muestra que la IA puede ayudar con el análisis forense de evidencia digital, incluidos registros del servidor, registros de tráfico de red, archivos del sistema y metadatos. Los algoritmos de inteligencia artificial pueden acelerar el proceso de análisis e identificar pistas importantes para los investigadores. Se utiliza para segmentar y clasificar diferentes tipos de amenazas cibernéticas según la gravedad, el origen y el método de ataque. Esto permite que los recursos de seguridad se asignen de manera más eficiente para abordar las amenazas más graves y urgentes. Los modelos de IA se pueden entrenar continuamente utilizando nuevos datos para adaptarse a los cambios en el panorama de las ciberamenazas.

Esto ayuda a las organizaciones a mantenerse informadas y mejorar sus defensas contra nuevos ataques. En algunos casos, la IA puede automatizar respuestas a incidentes de seguridad, como bloquear direcciones IP maliciosas, deshabilitar cuentas comprometidas y hacer cumplir políticas de seguridad en tiempo real. Los algoritmos de inteligencia artificial se pueden utilizar para analizar sistemas e identificar posibles vulnerabilidades de seguridad antes de que sean explotadas por piratas informáticos (Muñoz, 2023). Esto permite a las organizaciones tomar medidas proactivas para fortalecer sus defensas cibernéticas.

Pero la IA no es todo. Montes (2023) indica que es fundamental promover la educación en ciberseguridad y crear conciencia pública sobre los riesgos asociados con los delitos digitales. Esto puede incluir capacitación del personal, campañas de concientización pública y programas educativos en escuelas y universidades. El autor enfatiza la importancia de actualizar continuamente las leyes sobre ciberdelitos para seguir el ritmo de los avances tecnológicos y las tácticas criminales. Esto significa una disciplina más estricta y castigos más severos para quienes cometen delitos digitales. Las organizaciones y los gobiernos deben invertir en infraestructura y tecnología sólida de seguridad cibernética para proteger sus sistemas y datos de los ataques cibernéticos.

En consecuencia, la lucha contra la delincuencia digital requiere un enfoque integral que combine tecnologías innovadoras, cooperación internacional, legislación eficaz, educación pública y asociaciones público-privadas. La IA es una herramienta valiosa en este sentido, pero debe complementarse con muchas otras medidas para garantizar una defensa eficaz contra las ciberamenazas.

Realidad de la implementación de la IA en el Ecuador

Para Barragán (2023), la lucha contra la ciberdelincuencia en Ecuador enfrenta desafíos significativos en la adopción de tecnologías avanzadas como la inteligencia artificial (IA). A pesar del creciente reconocimiento del potencial de la IA para mejorar la eficacia en la detección y prevención de delitos cibernéticos, el país aún se encuentra en una etapa inicial en cuanto a la implementación de estas herramientas.

La adopción de IA en Ecuador ha sido limitada por varias razones. En primer lugar, las infraestructuras tecnológicas y de telecomunicaciones del país aún presentan deficiencias que dificultan el despliegue de soluciones avanzadas. Además, la formación y capacitación de talento especializado en IA y ciberseguridad es insuficiente, lo que limita la capacidad de las instituciones para utilizar estas tecnologías de manera efectiva (Velastegui, 2023). Comparado con otros países de la región, como Brasil o México, que han hecho avances significativos en la integración de IA en la ciberseguridad, Ecuador tiene mucho camino por recorrer (Barragán, 2023).

Recursos legales e institucionales existentes

El marco legal en Ecuador también presenta desafíos en cuanto a la regulación del uso de IA en la lucha contra la ciberdelincuencia. Las leyes actuales no contemplan de manera explícita las implicaciones del uso de tecnologías avanzadas como la IA, lo que genera vacíos legales que podrían afectar tanto la eficacia de las investigaciones como los derechos de las personas involucradas (Ponce, 2024).

Las instituciones encargadas de hacer cumplir la ley en Ecuador, como la Policía Nacional y la Fiscalía, carecen de los recursos necesarios para adoptar tecnologías de IA de manera amplia y efectiva (Dirección de Fomento de Tecnologías Emergentes, 2021). La falta de capacitación, infraestructura adecuada y colaboración interinstitucional son obstáculos que limitan la implementación de estas herramientas. Además, la cooperación internacional en

este ámbito es insuficiente, lo que restringe el acceso a tecnologías de vanguardia y a programas de capacitación especializados.

Métodos

Tipo de investigación: documental

El estudio inicia con una investigación documental como base primaria. Esta metodología es crucial porque permite fundamentar teóricamente la investigación mediante el análisis de documentos oficiales del Estado ecuatoriano, los cuales proporcionan estadísticas clave y antecedentes sobre la ciberdelincuencia en el país. Esta fase es esencial para entender el contexto y las dimensiones del problema, estableciendo una base teórica sólida.

Enfoque: enfoque descriptivo, no experimental

La investigación adopta un enfoque descriptivo, y observa el fenómeno de la ciberdelincuencia dentro de su contexto natural, sin intervención o manipulación de las variables. Este enfoque es importante porque permite reflejar fielmente la realidad actual del problema y cómo la integración de la inteligencia artificial podría influir en él. Al ser no experimental, el estudio se centra en la observación y descripción de los hechos tal y como se presentan.

Diseño de la investigación: transversal

Se emplea un diseño transversal que analiza los datos durante un periodo de diez años. Este diseño es relevante porque permite captar la evolución de la ciberdelincuencia en el tiempo, proporcionando una perspectiva amplia que es crucial para identificar tendencias y patrones.

Técnica de investigación

Entrevistas estructuradas

La recolección de datos se realizó por medio de entrevistas, lo cual es fundamental para obtener información directa y actualizada de expertos en la materia. Se diseñó un cuestionario estructurado con siete preguntas clave, enfocadas en dos áreas principales:

- **Estado actual de la ciberdelincuencia:** las primeras preguntas se centraron en analizar el estado actual de la ciberdelincuencia en Ecuador, desde la perspectiva de los expertos. Ello es crucial para obtener una visión interna y especializada sobre el problema.
- **Integración de inteligencia artificial:** posteriormente, se abordaron posibles soluciones a las falencias detectadas, explorando cómo la inteligencia artificial podría ser integrada en el manejo actual de la ciberdelincuencia. Este aspecto es esencial para identificar oportunidades de mejora en las estrategias actuales y proponer enfoques innovadores.

Selección de entrevistados

Para el estudio se utilizó una muestra y selección por conveniencia; se aplicó un muestreo estadístico, ya que se seleccionó a cinco policías que trabajan en la Unidad Nacional de Ciberdelito de la Policía Nacional del Ecuador. La selección por conveniencia fue deliberada para asegurar que los entrevistados fueran expertos con experiencia directa en el área de estudio.

Confidencialidad

Por razones de privacidad, los entrevistados serán citados como "entrevistados" en los resultados. Este aspecto es crucial para proteger la identidad y asegurar la confidencialidad de los participantes, respetando los principios éticos de la investigación. Además, al mantener el enfoque en sus puntos de vista y experiencia profesional, se garantiza que la información obtenida sea relevante y centrada en el trabajo investigativo.

Procedimiento para la recopilación de información

La entrevista se realizó mediante un cuestionario estructurado, que se envió inicialmente a los entrevistados por correo electrónico para que pudieran revisarlo y prepararse con anticipación. Posteriormente, según la disponibilidad de cada agente, se llevaron a cabo entrevistas en persona para profundizar en las respuestas y aclarar cualquier duda. Se eligió este enfoque mixto (entrevistas por correo electrónico y presenciales) para maximizar la flexibilidad y garantizar que los expertos pudieran contribuir de manera detallada, sin restricciones de tiempo o logística.

Una vez recopiladas todas las respuestas, se llevó a cabo un análisis exhaustivo de la información. Se seleccionaron las respuestas más relevantes y alineadas con los objetivos del estudio, asegurando que el análisis final reflejara los puntos de vista más significativos y que aportaran mayor valor al tema investigado. Esta selección fue necesaria para evitar una sobrecarga de información y para enfocar el estudio en aspectos clave

de la integración de la inteligencia artificial en la lucha contra la ciberdelincuencia.

Además, se elaboró un resumen de todas las respuestas obtenidas, con el fin de proporcionar un punto de vista objetivo y consolidado para cada pregunta del cuestionario. Este resumen permite identificar patrones comunes y destacar diferencias críticas en las opiniones de los expertos, ofreciendo una visión equilibrada y fundamentada para el análisis posterior.

Resultados

La información proporcionada por los policías de la Unidad Nacional de Ciberdelito de la Policía Nacional del Ecuador, mediante la entrevista, se ha condesado en los siguientes puntos:

1. Evaluación del estado actual de la ciberdelincuencia y los principales desafíos que enfrenta el país en este ámbito.

   Actualmente, el Estado ecuatoriano enfrenta desafíos significativos en cuanto a la seguridad de la información en línea. La carencia de herramientas que garanticen la seguridad, la confiabilidad y la fiabilidad ante las amenazas cibernéticas genera vulnerabilidades en diversos ámbitos, desde el usuario individual hasta las grandes empresas con una amplia infraestructura personal. Esta situación propicia el robo de información sensible, incluyendo documentación, bases de datos, información bancaria y credenciales de acceso a redes sociales, lo que puede desencadenar casos de acoso, extorsión y otras formas de delitos cibernéticos.

   El principal desafío radica en abordar el robo de información, tanto de naturaleza financiera como personal, que a menudo conduce a situaciones de extorsión. Para ello, es crucial implementar medidas de seguridad efectivas que puedan detectar y prevenir prácticas como el *phishing*, la clonación de documentos y garantizar la seguridad y el manejo adecuado de contraseñas y correos electrónicos. Sin dejar de lado la proliferación de las redes sociales, las cuales representan un riesgo significativo, especialmente para los menores de edad, quienes pueden ser víctimas de acoso, pedofilia y chantaje.

2. Principales tendencias y tipos de ciberdelitos.

   En este punto, los expertos mencionaron que el delito conocido como *grooming* se ha convertido en una preocupación creciente para las autoridades policiales, ya que los perpetradores aprovechan el uso de herramientas tecnológicas para contactar y manipular a menores de edad a través de plataformas diseñadas para niños, como los juegos en línea. Asimismo, la suplantación de identidad es una táctica común utilizada para obtener acceso a información personal sin control, incluyendo fotografías personales y laborales, que luego son manipuladas con el objetivo de obtener algún beneficio a costa de la reputación y la imagen de la víctima.

   Otros delitos frecuentes son el robo de información o directorios personales para generar estafas en línea, creando noticias falsas con el fin de alarmar a las personas, generando preocupación para luego extorsionar. En la misma línea, también se tiene la clonación de documentos como los comprobantes bancarios o de transferencias. Otro aspecto importante es la violación de propiedad intelectual, así como el monitoreo e intercepción de información emitida por instituciones como el sistema de emergencias ecuatoriano, conocido como el ECU 911, el cual se lleva a cabo mediante el uso de dispositivos sensores que se infiltran en las trasmisiones de información para su posterior uso en actividades delictivas.

3. Persistencia de las deficiencias tecnológicas en la detección y prevención de delitos cibernéticos en el Ecuador, a pesar del avance de la tecnología a nivel global.

   Los expertos exponen que el crecimiento exponencial de la tecnología en el país es indudable. No obstante, esta realidad presenta un desafío constante en cuanto a la seguridad de información. A medida que avanzan las innovaciones tecnológicas, es crucial desarrollar, a la par, herramientas que puedan contrarrestar las amenazas emergentes. Sin embargo, el mal empleo de las herramientas de seguridad actuales por desconocimiento o mala configuración, sumado a falta de explotación total de los distintos recursos y programas que se encuentran a la mano, limita la seguridad.

   El país precisa explotar de forma global y total los recursos para aprovechar todas las funcionalidades; sin embargo, la falta de personal especializado en el desarrollo de aplicaciones eficientes representa un obstáculo significativo. La capacitación y formación en áreas específicas son limitadas y restringidas; en consecuencia, existe personal capacitado, pero centrado a ciertas funciones únicas de diseño de *apps*, excluyendo netamente toda estrategia preventiva. Lo que ha provocado que el personal entre en una zona de confort, enfocando su trabajo

al cumplimiento de tareas diarias, pero sin invertir sus talentos en diseño de estrategias y programas que protejan la información y eviten el robo de esta.

4. Existen obstáculos específicos fuera de los económicos que enfrentan los organismos encargados de hacer cumplir la ley en la adopción e implementación de tecnologías avanzadas, como la inteligencia artificial.
   Al respecto, se observa que, fuera de los obstáculos económicos, la adopción e implementación de tecnologías avanzadas radica en la falta de personal especializado en áreas específicas, como en las fuerzas policiales, la Fiscalía y el Consejo de la Judicatura. Esta falta de conocimientos técnicos adecuados dificulta la implementación efectiva de soluciones tecnológicas avanzadas.
   Además, está el desconocimiento de las herramientas tecnológicas como tal. Esto es relevante, dado que muchas autoridades carecen de comprensión sobre las nuevas modalidades delictivas, y como resultado, no priorizan la inversión en tecnología de vanguardia, considerándola más como un gasto que como una inversión en seguridad.

5. Considera oportuna la colaboración internacional en la lucha contra los ciberdelitos en el Ecuador, especialmente en términos de acceso a recursos tecnológicos como la IA y capacitación especializada en esta herramienta.
   La colaboración internacional desempeña un papel fundamental en la lucha contra los ciberdelitos en Ecuador, especialmente en lo que respecta al acceso a recursos tecnológicos y la capacitación especializada en herramientas como la IA. Los ciberdelincuentes operan sin fronteras en el ciberespacio, lo que hace esencial la cooperación entre países para compartir información, coordinar investigaciones y desarrollar estrategias conjuntas para combatir estas amenazas.
   Aunque existen colaboraciones internacionales, como el apoyo de organismos de *Homeland Security Investigations* (HSI) y fundaciones como *OUR*, así también compromisos internacionales (Convenio de Budapest), estas no son suficientes para abordar plenamente las necesidades del país en este campo. Es necesario un mayor apoyo y una colaboración más constante y directa con países desarrollados y organizaciones internacionales para fortalecer las capacidades del Ecuador en la lucha contra los ciberdelitos.

6. ¿Qué medidas sugiere para mejorar la capacidad de respuesta y prevención de estos crímenes en el país?
   En primer lugar, se propone fortalecer el marco legal y regulatorio, así como establecer protocolos claros para la actuación en casos de cibercrimen, incluyendo el uso de figuras como el agente encubierto digital y la incautación de monedas digitales.
   Además, se destaca la importancia de invertir en tecnología y capacitación, tanto para el personal encargado de hacer cumplir la ley como para la ciudadanía en general, con el propósito de aumentar la conciencia pública sobre los riesgos cibernéticos y promover una cultura de mejorar la coordinación internacional. Conjuntamente, apoyar la colaboración entre diferentes instituciones gubernamentales y el sector privado, así como de establecer políticas de prevención constante y un monitoreo continuo del flujo de datos con personal capacitado y dedicado exclusivamente a la seguridad informática.
   En este sentido, la implementación de un Centro de Operaciones de Red (NOC) con un equipo especializado en la supervisión y respuesta a posibles amenazas cibernéticas, se presenta como medida clave para prevenir y mitigar los daños ocasionados por delitos cibernéticos. Este NOC estaría netamente encargado de controlar el flujo de información crítica destinada a instituciones financieras, sistemas de seguridad y otras herramientas tecnológicas, utilizando herramientas avanzadas como la IA para el reconocimiento facial y la generación de alertas.

7. ¿Cómo podría la implementación de tecnologías basadas en inteligencia artificial mejorar la eficacia de las investigaciones y la identificación de delitos cibernéticos en el Ecuador?
   La implementación de tecnologías basadas en inteligencia artificial (IA), podría significar un avance considerable en la mejora de la eficacia de las investigaciones y la identificación de delitos cibernéticos en Ecuador que se cometen por medio de la internet, *dark net* y *deep web*. Estas tecnologías permitirían un análisis más rápido y preciso de grandes volúmenes de datos, facilitando la detección de patrones y anomalías en el tráfico de red, lo que podría revelar actividades delictivas como ataques cibernéticos o intentos de fraude. Además, la IA podría simplificar y agilizar tareas monótonas en la investigación, como el análisis de

registros de actividad y la clasificación de evidencia digital, permitiendo a los investigadores dedicar más tiempo a actividades estratégicas y de mayor complejidad.

Otra contribución importante de la IA es su potencial para crear redes neuronales alimentadas con datos relevantes sobre delitos cibernéticos, lo que mejoraría significativamente la capacidad de predicción y prevención de futuros ataques, permitiendo una respuesta más rápida y eficiente ante las amenazas emergentes.

8. ¿Qué propuestas concretas podrían ofrecerse al legislador para fortalecer el marco normativo y garantizar que la inteligencia artificial se utilice de manera efectiva y ética en la lucha contra la ciberdelincuencia en Ecuador?

   Los entrevistados consideran crucial que el Estado desarrolle una ley específica para regular el uso de la inteligencia artificial (IA) en la lucha contra la ciberdelincuencia en Ecuador. Esta legislación debe establecer claramente los límites y responsabilidades en el uso de la IA, asegurando que su aplicación se centre en la prevención y combate de delitos cibernéticos, siempre respetando los derechos de los ciudadanos. Además, es imprescindible que se fortalezcan los programas de formación continua para los agentes, garantizando que comprendan y manejen estas tecnologías de manera ética y efectiva.

   También consideraron significativa la creación de unidades especializadas en IA en la Policía Nacional para apoyar al equipo que existe en la Unidad de Seguridad Cibernética, para enfrentar las crecientes amenazas en línea. Al mismo tiempo, es necesario actualizar el marco legal existente para incluir disposiciones que protejan los derechos procesales y la privacidad de los ciudadanos en el contexto de la ciberseguridad.

9. ¿Cuáles son los principales desafíos legales y procedimentales que enfrentan las autoridades en Ecuador al utilizar la inteligencia artificial en la recopilación de pruebas y el enjuiciamiento de delitos cibernéticos, y cómo podrían estas dificultades afectar la reparación de las víctimas?

   Se pudo evidenciar un consenso entre las respuestas de los oficiales, donde se indica que uno de los principales obstáculos para combatir eficazmente la ciberdelincuencia en Ecuador es la falta de un marco legal sólido y actualizado para el uso de la IA en específico. Dado que la ausencia de normas específicas sobre la admisibilidad de pruebas digitales obtenidas mediante inteligencia artificial podría generar incertidumbre jurídica y podría dificultar el enjuiciamiento de los cibercriminales. Casos emblemáticos como el hackeo al Banco del Pichincha en el 2021, donde se perdieron millones de dólares, evidencian las consecuencias de esta carencia legal. Incluso, en la actualidad, un elevado porcentaje de denuncias por ciberdelitos quedan impunes debido a estas limitaciones. Los entrevistados expertos en la materia coinciden en señalar que la falta de capacitación especializada en ciberseguridad y la ausencia de protocolos claros para el uso de las pruebas digitales en las investigaciones son factores agravantes. Es imperativo desarrollar una legislación integral que brinde un marco jurídico sólido para la lucha contra la ciberdelincuencia, garantizando así la protección de los derechos de las víctimas y la eficacia de las investigaciones si se va a utilizar la IA como herramienta contra estos delitos.

Discusión de resultados

La ciberdelincuencia representa uno de los desafíos más urgentes para Ecuador en el ámbito de la seguridad informática. La evaluación del estado actual, por parte de los entrevistados y las estadísticas consultadas sobre esta problemática, revelan una serie de vulnerabilidades que afectan a diferentes sectores, desde usuarios individuales hasta grandes empresas. Entre los principales ciberdelitos se identificaron el robo de información sensible, la proliferación de prácticas delictivas como el *phishing* y la suplantación de identidad, así como el uso inapropiado de las redes sociales. Esto no solo expone a los usuarios, especialmente a los menores de edad, a situaciones de acoso y chantaje, sino que también expone a toda la población a noticias que contienen *malware* en los enlaces de búsqueda.

Otro factor significativo es la falta de actualización por parte de las entidades de control y cumplimiento de las leyes. Se evidenció que existe personal capacitado generalmente para cumplir con las tareas diarias de monitoreo. Sin embargo, existen restricciones y limitaciones para capacitar a los policías en áreas específicas de prevención y diseño de estrategias de protección contra la ciberdelincuencia.

Por otra parte, se patentizó que la integración de la inteligencia artificial (IA) en la lucha contra la ciberdelincuencia es bien recibida. Puesto que permite crear redes de inteligencia y monitoreo en tiempo real y provee al servidor de protección la capacidad de analizar grandes cargas de información, identificando patrones y anomalías. En consecuencia, su funcionamiento no solo

radica en el análisis, sino que también puede establecer acciones preventivas, de detección en tiempo real y, en caso de llegar a suceder una infiltración, solventar brevemente las pérdidas y la recuperación del sistema.

Para abordar los desafíos en la lucha contra la ciberdelincuencia, es crucial que el legislador establezca una ley específica que regule el uso de la inteligencia artificial (IA) en ciberseguridad. Esta legislación debe definir claramente los límites y responsabilidades del uso de IA, asegurando su efectividad en la prevención y combate de delitos cibernéticos mientras protege los derechos de los ciudadanos. La falta de un marco legal actualizado sobre la admisibilidad de pruebas digitales genera incertidumbre jurídica y complica el enjuiciamiento de los cibercriminales, como se evidenció en los diferentes delitos cibernéticos presentados en el desarrollo del presente estudio y en la respuesta de los expertos en la entrevista. Además, es fundamental fortalecer la capacitación de los agentes y considerar la creación de unidades especializadas en IA en la Policía Nacional. La implementación de una normativa integral es esencial para garantizar una respuesta efectiva contra la ciberdelincuencia y evitar que un elevado porcentaje de denuncias quede impune.

Integración de la IA para mejorar los procesos de lucha contra los ciberdelitos en Ecuador

Con base en la información consultada y los resultados obtenidos de las entrevistas, en este apartado se presenta el análisis de la integración de la inteligencia artificial (IA) para combatir la ciberdelincuencia en el Ecuador.

Recuperación del sistema

En primer lugar, al analizar los casos de ciberataques en el país, tanto a entidades públicas como privadas, se comprobó que muchas de las entidades tuvieron un periodo de más de 48 horas en recuperarse del ataque cibernético, perdiendo información y acarreando problemas económicos. Por esta razón, se examina la IA como herramienta de recuperación frente a ciberataques, la cual tendría las siguientes ventajas:

Un sistema que se ejecute junto con IA proporcionaría a los usuarios la capacidad de reinstalar plataformas y programas afectados por el ataque, restaurando la funcionalidad del sistema. Además, permitiría al usuario iniciar la restauración de las copias de seguridad de la información y las aplicaciones, permitiéndole volver a un estado anterior al ataque.

Esta función se basa en tres pilares: la restauración de la integridad del sistema, guiada a volver a un estado de seguridad no comprometido; la restauración de la integridad de la información, enfocada a comprobar la información almacenada o procesada, verificando su integridad y cooficialidad; y por último, la trazabilidad de la información comprometida, dedicada específicamente a generar registros de toda la información que fue comprometida en el ataque para poder informar de manera efectiva a todas las partes interesadas (Portillo et al., 2022).

Inteligencia de amenazas

Los resultados de las entrevistas revelaron la necesidad de combatir diferentes tipos de ciberdelitos, con especial énfasis en la prevención de los ataques. Esta responsabilidad no debe recaer únicamente en las entidades de control y cumplimiento de la ley, sino que también debe involucrar a la comunidad en general. Sin embargo, la falta de una cultura de protección de datos entre la ciudadanía y el alto nivel de ataques que reciben las entidades y empresas, convierten a la inteligencia artificial en una herramienta para facilitar y fortalecer los procesos de protección.

La IA automatiza la recopilación de datos de diversas fuentes, como plataformas de código abierto, foros de la *dark web*, redes sociales o informes de seguridad. Esto permite a las organizaciones tener una visión completa del panorama de amenazas y comprender mejor cómo operan los actores maliciosos (Cisco, 2023). Adjunto a este proceso, la IA detecta los indicadores de compromiso (IOC), como direcciones de IP, dominios o *hashes* maliciosos, con mayor rapidez y precisión que los métodos manuales. Esta capacidad permite detener los ataques antes de que se materialicen.

Posteriormente, la IA puede programarse para analizar y generar registros históricos de ataques, lo que permite identificar patrones y, en consecuencia, predecir la probabilidad y el impacto de futuros ataques. Esta información proporciona a las organizaciones un marco para desarrollar estrategias preventivas y tomar medidas antes de sufrir un incidente.

En el contexto de la Unidad Nacional de Ciberdelito de la Policía Nacional del Ecuador, la implementación de herramientas de SEO (*search engine optimization*) para evaluar el impacto social de los enlaces podría ser una solución viable. Estas herramientas permitirían identificar amenazas de datos en una etapa temprana y establecer un sistema de monitoreo constante y remoto. Este sistema, dirigido por un Centro de Operaciones de Red (NOC), podría predecir casos y activar interruptores críticos para prevenir futuros incidentes.

Sin embargo, el monitoreo en tiempo real de alertas generadas por la implantación de virus y el comportamiento de *trolls* en línea, es fundamental para una respuesta efectiva ante las amenazas cibernéticas.

El desarrollo de herramientas de aprendizaje predictivo permitiría anticipar y contrarrestar estas amenazas de manera proactiva, garantizando la seguridad del ciberespacio ecuatoriano.

Análisis de malware

Según los datos de Kaspersky, los delitos por *malware* alcanzan a 18 millones. El portal expone la existencia de diversos tipos de ciberdelincuencia vinculados a este tipo de ataque, y posiciona a Ecuador como el quinto país en Sudamérica que más lo recibe a diario. Por tanto, es fundamental implementar acciones contra el malware antes de que ingrese al sistema (Kaspersky, 2024).

Y es en esta faceta que la IA se convierte en una herramienta esencial para la prevención de ciberataques. Este proceso implica la examinación, la comprensión del comportamiento y la identificación de las características del software malicioso.

En primer lugar, se identifican y comprenden los diferentes tipos de *malware*. Una vez identificados, la IA tiene la facilidad de descompilar el código del *malware*, extrayendo información crucial como el tipo, su funcionalidad, origen y objetivo (Cisco, 2023). Con esta información, la herramienta ya puede atribuir ataques a hackers específicos. Mediante su procesamiento de lenguaje natural (PLN), analiza las notas de rescate o los canales de comunicación de los atacantes para determinar su identidad, idioma o ubicación.

Finalizando en el proceso, como último paso, la IA clasifica y detecta las variantes de *malware*. Su aprendizaje automático de *machine learning* (ML) analiza e interpreta patrones y estructuras de datos, lo que permite la detección de similitudes o variaciones entre ellas. De esta manera, la IA crea un modelo de aprendizaje automático y toma decisiones basadas en la experiencia del algoritmo. Esto la convierte en una herramienta extremadamente útil en situaciones donde la presencia humana no es posible o el acceso está restringido (Cisco, 2023).

Respuesta a incidentes

En la actualidad, el proceso de respuesta a incidentes cibernéticos está bajo la responsabilidad de EcuCERT en conjunto con la Agencia de Regulación y Control de las Telecomunicaciones (Arcotel). Los informes estadísticos de la entidad detallan el número de IP notificadas como vulnerables, por incidentes reportados, reportes de fraudes y la capacitación brindada al personal. No obstante, el servicio de protección no está disponible para toda la población. Este servicio se ofrece bajo demanda a instituciones públicas, a través de la gestión documental Quipux, con la solicitud al director de Control de Servicio de Telecomunicaciones (EcuCERT, 2024).

El proceso de análisis actual se desarrolla en dos fases:

a. El monitoreo continuo: personal capacitado realiza un monitoreo constante para detectar cualquier anomalía.
b. Evaluación de prioridad: si se detecta una alerta, se evalúa su prioridad utilizando el protocolo *Traffic Ligth Protocol* (TPL). Este protocolo asigna un código de color que indica la gravedad del incidente:

    - Rojo: crítica
    - Ámbar: alta
    - Verde: media
    - Blanco: baja

Es importante destacar que este código mide el nivel de diseminación del incidente, no su nivel de sensibilidad (EcuCERT, 2024).

En caso de detectarse una alarma, se ejecuta el escaneo de vulnerabilidades en conjunto con metodologías para la identificación de amenazas. Finalmente, se registran y envían informes de riesgos informáticos a la entidad solicitante. Como se detalla en la página oficial de EcuCERT (2024), el sistema actualmente funciona a nivel público para entidades gubernamentales. Sin embargo, esta realidad puede cambiar si se invierte en la integración de la IA en parte del proceso de gestión de trabajo de EcuCERT.

La IA desempeña un papel significativo en la prevención de ciberataques al facilitar la respuesta a incidentes. Este proceso, que abarca la contención, erradicación, recuperación y aprendizaje de un ataque para mejorar la seguridad, se ve potenciado por la IA por medio de:

- La automatización del análisis y priorización: la IA automatiza el análisis de los incidentes, priorizando aquellos que requieren atención inmediata. Esto libera al equipo de seguridad para que se concentre en tareas más complejas.
- Orientación y soporte al equipo de seguridad: la IA proporciona asistencia al equipo de seguridad y a los usuarios finales, ofreciendo instrucciones sobre cómo responder al ataque, cómo cambiar contraseñas, restaurar copias de seguridad o reportar el incidente de inmediato.
- Generación de informes y paneles: la herramienta utiliza el análisis y la visualización de datos para generar informes y paneles que resuman los detalles y resultados del incidente, junto con recomendaciones para mejorar la seguridad (Portillo et al., 2022).

Propuestas para el legislador y la doctrina

Para superar estos desafíos, es necesario un enfoque integral que involucre tanto la actualización del marco legal como el fortalecimiento de las capacidades institucionales. En términos legislativos, se sugiere la creación de una ley específica que regule el uso de la IA en la ciberseguridad, garantizando que su aplicación sea ética y respetuosa de los derechos humanos. Esta ley debería abordar aspectos clave como la privacidad de los datos, la responsabilidad en el uso de tecnologías de IA, y los criterios para la admisibilidad de pruebas obtenidas mediante estas herramientas en procesos judiciales.

Desde el punto de vista doctrinal, es fundamental desarrollar principios éticos y directrices para el uso de la IA en la ciberseguridad. Estos principios deberían guiar tanto a los profesionales del derecho como a los encargados de la seguridad en el uso responsable de estas tecnologías. Además, es crucial fomentar la colaboración entre el Gobierno, las universidades y el sector privado para impulsar la investigación y el desarrollo de soluciones de IA adaptadas a las necesidades específicas de Ecuador.

Finalmente, es imperativo que el Estado ecuatoriano promueva una mayor cooperación internacional en el ámbito de la ciberseguridad, participando activamente en iniciativas globales que permitan el intercambio de conocimientos y tecnologías. La implementación exitosa de IA en la lucha contra la ciberdelincuencia, no solo mejorará la capacidad del país para enfrentar estos delitos, sino que también fortalecerá la protección de los derechos de los ciudadanos en el entorno digital.

Por consiguiente, se demuestra que la IA se convierte en un recurso invaluable para la prevención de ciberataques en el país. Facilita la respuesta a incidentes virtuales, la prevención de infiltraciones mediante la automatización e interpretación de grandes caudales de datos, lo que permite la identificación certera del tipo de *malware* que ataca el sistema. Posteriormente, posibilita la recuperación y minimización de daños luego de un ataque cibernético.

Conclusiones

Al evaluar la situación actual del Ecuador con relación a la ciberdelincuencia, se constata que el país enfrenta grandes desafíos en cuanto a su seguridad virtual. Existen vulnerabilidades en diferentes sectores, desde el nivel de los ciudadanos individuales hasta grandes empresas y entidades gubernamentales. Entre los principales ciberdelitos que ocurren en el territorio ecuatoriano, el robo de información sensible, el *phishing* y la suplantación de identidad son los más comunes.

En cuanto al sector más vulnerable, al analizar los diferentes casos de ataques cibernéticos, se comprueba que el sector público es el más propenso a sufrir hackeos, con el propósito principal de secuestrar datos y la falsificación de documentos. Lamentablemente, las entidades gubernamentales cuentan con poca infraestructura tecnológica, lo que dificulta la protección de sus sistemas. Sin embargo, es destacable que, posterior a los ataques sufridos en los últimos años, se han creado nuevas entidades como la EcuCERT y se han establecido convenios con países extranjeros con el propósito de mitigar estos problemas.

Respecto a la integración de la inteligencia artificial en la lucha contra la ciberdelincuencia, se confirma que el panorama es altamente positivo. Esta herramienta puede ser utilizada en diferentes ámbitos de aplicación e investigación, especialmente en áreas de recuperación de sistemas, la inteligencia de amenazas, el análisis de *malware* y la respuesta a incidentes. Gracias a sus sistemas automatizados, la IA es altamente eficiente en el análisis de grandes bases de datos, lo que contribuye a un monitoreo en tiempo real de estos problemas. Por consiguiente, el Ecuador fortalecería sus sistemas de protección contra los ciberdelincuentes.

Conflicto de interés

No se presentó conflicto de interés en el desarrollo de la presente investigación académica. Declaro que no tengo ninguna relación financiera o personal que pudiera influir en el diseño de los experimentos realizados, así como la interpretación y publicación de los resultados obtenidos. Asimismo, aseguro cumplir con las normas éticas y de integridad científica en todo momento, de acuerdo con las directrices establecidas por la comunidad académica y las dictaminadas por la presente revista.

Referencias

Abrams, L. (2021). *Ecuador's state-run CNT telco hit by RansomEXX ransomware*. Bleeping Computer. https://www.bleepingcomputer.com/news/security/ecuadors-state-run-cnt-telco-hit-by-ransomexx-ransomware/

Acaro, H. (2023). *Análisis de la influencia de los ciberataques para la generación de políticas públicas en el Ecuador en el ámbito de la gobernanza del Internet*. [Tesis, Universidad Nacional de Loja]. https://dspace.unl.edu.ec//handle/123456789/27124

Albors, J. (2020). *Qué es un ataque de fuerza bruta y cómo funciona*. WeLiveSecurity. https://www.welivesecurity.com/la-es/2020/06/24/que-es-ataque-fuerza-bruta-como-funciona/

ANT. (2021). *La ANT informa sobre ataque cibernético a sus sistemas*. Agencia Nacional de Tránsito del Ecuador (ANT).

Barragán-Martínez, X. (2023). Situación de la inteligencia artificial en el Ecuador en relación con los países líderes de la región del Cono Sur. *FIGEMPA: Investigación y Desarrollo*, *16*(2), 23-38. https://doi.org/10.29166/revfig.v16i2.4498

Bravo, J. C., Márquez, D. M., Cavero, A. V. y Antúnez, J. O. (2021). La influencia de la automatización inteligente en la detección del cibercrimen financiero. *Boletín de Coyuntura*, *31*, 26-33. https://doi.org/10.31243/bcoyu.31.2021.1462

CCN-CERT. (2023). *Informe de buenas prácticas BP/30 sobre aproximación a la inteligencia artificial y la ciberseguridad*. Centro Criptológico Nacional. https://www.ccn-cert.cni.es/es/seguridad-al-dia/novedades-ccn-cert/12852-nuevo-informe-de-buenas-practicas-bp-30-sobre-aproximacion-a-la-inteligencia-artificial-y-la-ciberseguridad.html

Cisco. (2023). *¿Cómo se puede utilizar la inteligencia artificial para prevenir los ciberataques?* https://es.linkedin.com/advice/3/how-can-artificial-intelligence-used-prevent-5hcjf?lang=es

Coello, N. (2021). *Análisis de ciberataques en organizaciones públicas del Ecuador y sus impactos administrativos*. Universidad Politécnica Salesiana. https://dspace.ups.edu.ec/bitstream/123456789/20738/1/UPS-GT003334.pdf

CSIRT-EPN. (2021). *Banco Pichincha sufre ciberataque*. https://www.csirt-epn.edu.ec/como-tener/225-ciberataque-banco-pichincha

Dávalos, N. (2021). *Los misterios del ataque que dejó a CNT sumida en la "emergencia"*. https://www.primicias.ec/noticias/tecnologia/los-misterios-del-ataque-que-dejo-a-cnt-sumida-en-emergencia/

Dirección de Fomento de Tecnologías Emergentes. (2021). *Diagnóstico sobre la inteligencia artificial en el Ecuador*. https://observatorioecuadordigital.mintel.gob.ec/wp-content/uploads/2022/11/Proyecto-diagnostico-inteligencia-artificial-IA-en-Ecuador-Documento-final-JC-JO-MS-002.pdf

DNTIC. (2020). *Delitos informáticos en Ecuador*. Departamento de Seguridad de las TIC.

Echeverría, D. (2024). *Crisis de seguridad en Ecuador: amenazas digitales y recomendaciones para mitigarlas*. https://www.linkedin.com/pulse/crisis-de-seguridad-en-ecuador-amenazas-digitales-y-echeverr%C3%ADa-mu%C3%B1oz-txpze/

EcuCERT. (2024). *Nosotros - EcuCERT de Arcotel*. https://www.ecucert.gob.ec/nosotros/

El Universo. (2023). Ecuador es uno de los tres países latinoamericanos con más ciberataques. *El Universo*. https://www.eluniverso.com/noticias/ecuador/ecuador-es-uno-de-los-tres-paises-latinoamericanos-con-mas-ciberataques-nota/

Esquivel, A. S. y Recalde, L. (2023). El Estado y la defensa del ciberespacio. *Revista de la Academia del Guerra del Ejército Ecuatoriano*, *16*(1). https://doi.org/10.24133/AGE.VOL16.N01.2023.07

FGE (Fiscalía General del Estado). (2021). El rol de la administración de justicia y la cooperación internacional en la lucha contra la ciberdelincuencia. *Revista Científica de Ciencias Jurídicas, Criminología y Seguridad*, *30*. https://www.fiscalia.gob.ec/pdf/politica-criminal/Ciberdelitos-Perfil-Criminologico.pdf

Forbes Ecuador. (2023). Cuatro tendencias de riesgo cibernético para observar en 2023. *Revista Forbes Ecuador*. https://www.forbes.com.ec/innovacion/cuatro-tendencias-riesgo-cibernetico-observar-2023-n27981

Freire, K. (2017). *Estudio y análisis de ciberataques en América Latina, su influencia en las empresas del Ecuador y propuesta de políticas de ciberseguridad*. Universidad Católica de Santiago de Guayaquil. http://repositorio.ucsg.edu.ec/bitstream/3317/9203/1/T-UCSG-PRE-TEC-ITEL-245.pdf

Fundamedios. (2024). *Portal de medio digital ecuatoriano sufre ataque cibernético*. https://www.fundamedios.org.ec/alertas/portal-de-medio-digital-ecuatoriano-sufre-ataque-cibernetico/

Gárate, K. (2023). *Principales vectores de ataque utilizados por ciberdelincuentes: vulnerabilidades y consejos de prevención*. https://www.linkedin.com/pulse/principales-vectores-de-ataque-utilizados-por-y-karen-g%C3%A1rate-ferj/

Gobierno Electrónico de Ecuador. (2019). *Principales ciberamenazas en Ecuador*. https://www.gobiernoelectronico.gob.ec/principales-ciberamenazas-en-ecuador/

Harán, J. (2021). *Banco Pichincha sufrió ataque informático que afectó parte de sus servicios*. https://www.welivesecurity.com/la-es/2021/10/14/banco-pichincha-sufrio-ataque-informatico/

Interpol. (2024). *Análisis forense digital*. https://www.interpol.int/es/Como-trabajamos/Innovacion/Analisis-forense-digital

Kaspersky. (2024). *Estadísticas | Mapa en tiempo real de amenazas cibernéticas*. https://cybermap.kaspersky.com/es/stats#country=35ytype=OASyperiod=w

Ley General de Protección de Datos. (s.f.). *Estadísticas | Mapa en tiempo real de amenazas cibernéticas*. https://cybermap.kaspersky.com/es/stats

Llangarí, A. M. (2016). *Análisis de los delitos informáticos y de telecomunicaciones en el Ecuador bajo las nuevas formas jurídicas*. [Tesis, Universidad de las Fuerzas Armadas ESPE. Carrera de Ingeniería Electrónica en Redes y Comunicación de Datos]. http://repositorio.espe.edu.ec/jspui/handle/21000/11654

Loor Campúes, F. D., Zambrano Rendón, A. D., Zambrano Vera, W. O. y Párraga Vera, R. G. (2023). *Delitos informáticos en tiempos de covid: revisión literaria Ecuador*. https://www.espam.edu.ec/recursos/sitio/informativo/archivos/ponencias/vinculacion/i/s3/CIV52EIT24.pdf

MINTEL. (2022). *Diagnóstico de las capacidades de ciberseguridad*. Banco Mundial-Birf. https://n9.cl/aylb3

Montes Vallejo, C. F. (2023). *Inteligencia artificial y el aprendizaje automático en la ciberseguridad*. Universidad Piloto de Colombia. https://n9.cl/koafem

Montes, I. y Vergara, A. (2023). *Análisis de los ataques cibernéticos en la banca ecuatoriana: Mapeo sistemático*. Universidad Politécnica Salesiana.

Muñoz, A. (2023). *La importancia del análisis forense digital en la era tecnológica*. https://www.linkedin.com/pulse/la-importancia-del-an%C3%A1lisis-forense-digital-en-era-mu%C3%B1oz-bermudez/

Ochoa, A. C. (2021). *Desafíos globales del cibercrimen: caso Ecuador período 2014-2019*. [Tesis, Universidad Andina Simón Bolívar]. http://repositorio.uasb.edu.ec/handle/10644/7919

Onofa, M. (2022). *Ataques cibernéticos amenazan seguridad en Ecuador*. https://dialogo-americas.com/es/articles/ataques-ciberneticos-amenazan-seguridad-en-ecuador/

Ponce, J. (2024). *Revisión: Ley Orgánica de Regulación y Promoción de la Inteligencia Artificial en Ecuador*. https://www.linkedin.com/pulse/revisi%C3%B3n-ley-org%C3%A1nica-de-regulaci%C3%B3n-y-promoci%C3%B3n-la-artificial-ponce-h18le/

Portillo, S., Martínez, J. y Mariadíaga, R. (2022). Ciberseguridad, inteligencia artificial y nuevas tecnologías en el área de defensa. En *XXIII Conferência de Direitos dos Colégios de Defesa Ibero-Americanos, agosto 22* (pp. 233-265). https://www.asociacioncolegiosdefensaiberoamericanos.org/images/Libros/Libro_2022.pdf

Rosero, J. (2021, octubre 22). Fiscalía investiga ataque cibernético a sistema informático de la ANT. *El Comercio*. https://www.elcomercio.com/actualidad/seguridad/fiscalia-investigacion-ataque-cibernetico-ant.html

Seguridad 360. (2021). Hackeo al Banco Pichincha afectó parte de sus servicios. *Revista Seguridad 360*. https://revistaseguridad360.com/noticias/hackeo-al-banco-pichincha/

Suastegui, L. (2022). *Estudio y análisis de ataques informáticos en Ecuador durante el estado de pandemia de COVID-19* [Universidad Católica de Santiago de Guayaquil]. http://repositorio.ucsg.edu.ec/bitstream/3317/18016/1/T-UCSG-PRE-TEC-ITEL-421.pdf

Tejedor, J. (2023). *Los vectores de ataque más utilizados por los ciberdelincuentes*. https://www.linkedin.com/pulse/los-vectores-de-ataque-m%C3%A1s-utilizados-por-jose-tejedor/

Velastegui, E. U. (2023). *Inteligencia artificial y su potencial adopción en los servicios públicos: desafíos y oportunidades en Ecuador a partir del período 2021-2022*. https://repositorio.puce.edu.ec/handle/123456789/43320