30

Fecha de presentación: marzo, 2024
Fecha de aceptación: julio, 2024
Fecha de publicación: septiembre, 2024

EFECTIVIDAD

DE LAS POLÍTICAS IMPLEMENTADAS PARA GARANTIZAR LA SEGURIDAD CIBERNÉTICA EN ECUADOR

EFFECTIVENESS OF THE POLICIES IMPLEMENTED TO GUARANTEE CYBERSECURITY IN ECUADOR

Vanessa Josefa Hernández Alvarado [1*]
E-mail: ub.vanessahernandez@uniandes.edu.ec
ORCID: https://orcid.org/0000-0002-9396-994X
Segundo Heriberto Granja Huacón [1]
E-mail: ub.segundogh04@uniandes.edu.ec
ORCID: https://orcid.org/0009-0007-6058-2478
Jeniffer Leonor Arias Hernández [1]
E-mail: db.jenifferlah05@uniandes.edu.ec
ORCID: https://orcid.org/0009-0001-9617-1749
[1] Universidad Regional Autónoma de Los Andes, Babahoyo. Ecuador.
*Autor para correspondencia

Cita sugerida (APA, séptima edición)

Hernández Alvarado, V. J., Granja Huacón, S. H. & Arias Hernández, J. L. (2024). Efectividad de las políticas implementadas para garantizar la seguridad cibernética en Ecuador. ***Universidad y Sociedad 16***(5), 288-296.

RESUMEN

La implementación de políticas de ciberseguridad es esencial para que los gobiernos protejan su información, salvaguarden la seguridad nacional, cumplan con sus obligaciones legales y normativas, y garanticen la prestación segura y continua de servicios públicos. La Política de Ciberseguridad de Ecuador está diseñada para proteger los activos digitales y la infraestructura crítica del país, no obstante existen múltiples manifestaciones de violaciones en cuanto a ciberseguridad. En este contexto, se hace necesario valorar la efectividad de las políticas implementadas para garantizar la seguridad cibernética en Ecuador, en consonancia con la evolución tecnológica y las amenazas emergentes. De forma mayoritaria el sistema es valorado como poco eficaz. Se identifican como brechas fundamentales la falta de coordinación entre instituciones gubernamentales y organismos encargados de la seguridad informática. Se requiere actualizar la legislación y la elaboración de guías de procedimiento que brinden orientación práctica a los operadores judiciales en el manejo de casos. El país debe continuar fortaleciendo su política nacional de ciberseguridad, promoviendo la colaboración público- privada, la innovación y la adopción de buenas prácticas de seguridad cibernética que faciliten la protección de la información sensible y la mitigación de riesgos cibernéticos.

Palabras clave: Seguridad cibernética, Tecnologías de la información y las comunicaciones, Entornos digitales, Delito informático, Ciberespacio.

ABSTRACT

Implementing cybersecurity policies is essential for governments to protect their information, safeguard national security, meet their legal and regulatory obligations, and ensure the safe and continuous delivery of public services. Ecuador's Cybersecurity Policy is designed to protect the country's digital assets and critical infrastructure, however there are multiple manifestations of cybersecurity violations. In this context, it is necessary to assess the effectiveness of the policies implemented to guarantee cybersecurity in Ecuador, in line with technological evolution and emerging threats. For the most part, the system is considered ineffective. The lack of coordination between government institutions and organizations in charge of computer security is identified as fundamental gaps. It is necessary to update the legislation and the development of procedural guides that provide practical guidance to judicial operators in the management of cases. The country must continue to strengthen its national cybersecurity policy, promoting public-private collaboration, innovation and the adoption of good cybersecurity practices that facilitate the protection of sensitive information and the mitigation of cyber risks.

Keywords: Cybersecurity, Information and communications technologies, Digital environments, Computer crime, Cyberspace.

INTRODUCCIÓN

La ciberseguridad, también conocida como seguridad informática o seguridad cibernética, se refiere a la protección de sistemas informáticos, redes, dispositivos y datos contra el acceso no autorizado, el robo, la manipulación o cualquier otro tipo de riesgos asociados a la tecnología de la información. Es un tema de vital importancia para la seguridad ciudadana y de los Estados, siendo una tendencia mundial, de la cual Ecuador no se encuentra aislado.

Esta disciplina engloba un conjunto de herramientas, políticas, prácticas y mecanismos diseñados para salvaguardar la integridad, confidencialidad y disponibilidad de la información en entornos digitales, por lo que promueve otros desarrollos digitales, como el comercio electrónico, la protección información y transacciones financieras, cuidado de los datos personales de los ciudadanos e información comercial a nivel local e internacional. Este término fue introducido a principios del 2011, por parte del grupo bilateral de trabajo del East West Institute y la Universidad de Moscú (Vidal, 2022).

Leiva (2015) define la ciberseguridad como una propiedad del ciberespacio, que tiene la capacidad de resistir las amenazas intencionales y no intencionales, responder y recuperarse. Para Caro (2010) es un conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, orientación, metodologías de gestión de riesgos, acciones, capacitación, mejores prácticas, seguros y tecnología que se pueden utilizar para proteger los activos y usuarios de una organización en una red.

El reconocimiento del derecho de acceso a internet en el ámbito de las Naciones Unidas se sitúa en dos momentos: en el año 2000, con la Declaración del Milenio, inicio de las agendas internacionales tendentes a la consecución de un acceso a internet equitativo, y en 2011, con el informe del relator especial de las Naciones Unidas sobre la promoción y la protección del derecho a la libertad de opinión y de expresión, en el que se reconoce que el derecho de acceso a internet, ligado a la libertad de expresión y comunicación, habría de ser un derecho humano garantizado por los Estados (Álvarez, 2022). A partir de aquí la revolución de las tecnologías de la información y las comunicaciones ha acelerado el proceso de globalización y periódicamente ha traído sorpresas.

El ciberespacio se ha convertido cada vez más en una nueva dimensión de la interacción social y, en consecuencia, ha surgido la ciberseguridad popular por su constante innovación. Un ejemplo es el aumento del número de dispositivos conectados al ciberespacio, que ha dado lugar a la llamada Internet de las Cosas (Sancho, 2017). En este entorno las técnicas de prevención ante ciberamenazas surgen como una alternativa para contrarrestar eventos maliciosos y además brindar a los usuarios herramientas que otorgan confianza para navegar en el ciberespacio (Cando & Medina, 2021).

En la era digital, la ciberseguridad es una preocupación fundamental para empresas, organizaciones gubernamentales, instituciones financieras, proveedores de servicios de tecnología y, en general, para cualquier entidad que haga uso de la tecnología de la información. Las amenazas cibernéticas, como el robo de datos, el ransomware, el phishing y otras formas de ataques maliciosos, hacen que la ciberseguridad sea una prioridad ineludible en el entorno actual de interconexión digital. En este sentido, la ciberseguridad y la creación de confianza en el ciberespacio se vuelven cruciales, como lo demuestra el papel de los Estados a la hora de afrontar el surgimiento de nuevas amenazas y controlar el ciberespacio (Méndez, 2021).

El ciberespacio ha pasado a interesar al Derecho en distintas ramas. La ciberseguridad, en consecuencia, ha sido regulada parcialmente por normas administrativas y penales, pero algunas implicaciones constitucionales resultan de extraordinaria importancia, como ha puesto de relieve el conjunto de medidas adoptadas por la pandemia, deviniendo insuficiente la previsión de planes y normas anteriores (Fernández, 2021).

De ahí que la implementación de políticas de ciberseguridad es esencial para que los gobiernos protejan su información, salvaguarden la seguridad nacional, cumplan con sus obligaciones legales y normativas, y garanticen la prestación segura y continua de servicios públicos. Asimismo, estas acciones contribuyen a mantener la confianza de los ciudadanos en las capacidades del gobierno para proteger sus datos y operar de manera segura y resiliente en el entorno cibernético actual.

Ecuador tiene la responsabilidad de responder a las ciberamenazas o ciberataques, proteger la infraestructura digital crítica, los servicios básicos nacionales, la infraestructura crítica de defensa digital, y proteger los datos personales y los derechos en el ciberespacio. Es por ello que la política nacional de ciberseguridad en tiene un marco estratégico establecido por el gobierno para abordar los desafíos y riesgos asociados con la seguridad en línea y la protección de la información digital, con implicaciones en la administración de justicia, incluyendo la legislación, la investigación y persecución de delitos cibernéticos, la protección de derechos y privacidad, y la

cooperación internacional en materia de ciberseguridad (Moncayo, 2019).

Los antecedentes históricos y jurídicos revelan una evolución del marco normativo en materia de ciberseguridad en Ecuador. Desde la promulgación de la Ley Orgánica de Comunicación en 2013 hasta la reciente aprobación de la Ley de Protección de Datos Personales en 2021, el país ha ido fortaleciendo su legislación para hacer frente a los desafíos que plantea el entorno digital. La actual política nacional de ciberseguridad aborda diversas teorías y enfoques relacionados con la protección de los sistemas de información y la gestión de amenazas cibernéticas a nivel nacional.

Sin embargo, a pesar de estos avances legislativos, persisten desafíos significativos en la administración de justicia en relación con la ciberseguridad. La falta de capacitación especializada de los operadores judiciales, la escasez de recursos tecnológicos y la complejidad de los delitos informáticos son solo algunas de las problemáticas que obstaculizan la eficacia del sistema judicial en este ámbito.

El Estado ecuatoriano en su Constitución Política, como norma jurídica fundamental, considera la responsabilidad de desarrollar políticas que protejan los derechos de las personas, en este caso, para brindar protección al uso del ciberespacio. En el país, los ciberdelitos están tipificados en el Código Orgánico Integral Penal (COIP) como una medida para perseguirlos y fijar sanciones. Actualmente, el Ecuador cuenta con Leyes que condenan esta clase de delitos con penas de privación de libertad, los mismos que permanecen identificados en el COIP. El delito informático está tipificado en el artículo 190 de este cuerpo normativo.

Desde la entrada en vigor del COIP se ha registrado un aumento significativo en el número de denuncias presentadas en la Dependencia Estatal de la Fiscalía General del Estado, por intermedio del Servicio de Atención Integral (Méndez, 2021). Por lo tanto, para lograr un Ecuador digitalmente seguro que garantice el Estado de Derecho, proteja la infraestructura y los servicios críticos del país y la seguridad de la población en el ciberespacio, es necesario desarrollar recomendaciones de ciberseguridad aplicables a los procedimientos de justicia digital.

Ecuador enfrenta desafíos en materia de ciberseguridad, incluyendo la protección de la infraestructura crítica, la prevención de ciberataques, la gestión de incidentes y la preparación ante amenazas emergentes, como el ransomware y el cibercrimen. Como respuesta a estos desafíos, el país ha emitido regulaciones jurídicas en pos de garantizar la seguridad cibernética. No obstante persisten brechas, ya que como en otros países, existen múltiples manifestaciones de violaciones en cuanto a ciberseguridad.

En este contexto, se hace necesario valorar la efectividad de las políticas implementadas para garantizar la seguridad cibernética en Ecuador, en consonancia con la evolución tecnológica y las amenazas emergentes.

MATERIALES Y MÉTODOS

El presente artículo científico se basa en una investigación de tipo cualitativo, que combina el análisis documental con entrevistas y cuestionarios como métodos de recolección de datos.

Los métodos de nivel teórico que se emplearon en el presente artículo científico son:

- Deductivo-Inductivo: Se aplicó en el estudio de la Constitución de la República del Ecuador, Ley Orgánica de Comunicación, Ley de Protección de Datos Personales, Código Orgánico Integral Penal y las Políticas de Ciberseguridad vigentes, para poder entender la normativa particular con respecto a la Política Nacional de Ciberseguridad y su efectividad en el Ecuador.
- Analítico – sintético: Se aplicó en el análisis de las normas, la doctrina y la jurisprudencia, para valorar la problemática estudiada, aplicando el método sintético en la descomposición llevada a efecto por el método analítico.
- Histórico-Lógico: Método mediante el cual se logró recopilar los antecedentes históricos de la Política Nacional de Ciberseguridad implementados .

Las técnicas de recolección de datos que se emplearon son:

- Encuesta: Constituye una técnica de gran importancia para la investigación porque permite recabar los datos de la población implicada a través de la utilización de un formato pre establecido conformado de preguntas de tipo cerradas. Se aplicó a 89 profesionales del Derecho en libre ejercicio de la profesión del Foro de Abogados de Los Ríos.
- Revisión documental: Se utilizó en la aplicación de diversas fuentes bibliográficas de autores nacionales y extranjeros.

Instrumento de recolección de datos: Cuestionario.

La población seleccionada para llevar a efecto esta investigación es de 1600 profesionales de Los Ríos, obteniéndose una muestra de 89 profesionales de derecho

que ejercen como jueces, fiscales, abogados especializados en derecho digital y funcionarios de organismos gubernamentales encargados de la seguridad informática.

Como indicadores de inclusión se consideraron:

- Pertenencia al gremio de profesionales de derecho del Colegio de Abogados de Los Ríos de la ciudad de Babahoyo, en ejercicio de la profesión, ya sea como jueces, fiscales, abogados expertos en derecho digital.
- Funcionarios de organismos gubernamentales administradores de la seguridad informática.
- Poseer experiencia y conocimientos relevantes en el tema objeto de estudio.

Como variable objeto de estudio se definió la implementación de la Política nacional de ciberseguridad. En la tabla 1 se muestra la operacionalización de la misma.

Tabla 1: Operacionalización de las variables de la investigación.

Variable	Definición de la variables	Dimensiones	Indicadores	Instrumentos	Grado de realización del indicador	Unidades de análisis
Implementación de la Política nacional de ciberseguridad	Normas cuya aplicación permiten regular el funcionamiento en el área cibernética con el objetivo de promover un ciberespacio libre, abierto, seguro y resiliente.	Legislación	Capacidad de respuesta a incidentes.	Encuesta	Escala	Cantón Babahoyo Provincia Los Ríos.
		Regulación	Educación en ciberseguridad	Entrevista		
				Revisión documental		

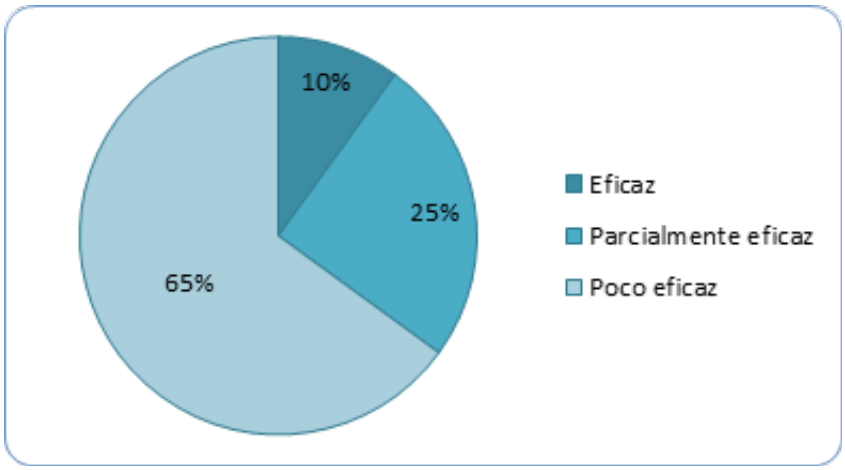
Fuente: Elaboración propia.

RESULTADOS Y DISCUSIÓN

Resultados de la aplicación de la encuesta a profesionales de Derecho entre ellos jueces, fiscales y abogados expertos en Derecho Digital. La misma se estructuró con 3 preguntas, enfocadas en valorar el grado de eficacia, desafíos que enfrenta la implementación de la Política Nacional de ciberseguridad y posibles soluciones para enfrentarlos, ver figuras 1,2 y 3, Los resultados cualitativos de cada una se muestran en las tablas 1, 2 y 3 respectivamente.

Pregunta 1: Cuál es su percepción sobre la eficacia de la Política nacional de ciberseguridad?

Fig 1: Resultados de la pregunta 3 de la encuesta.

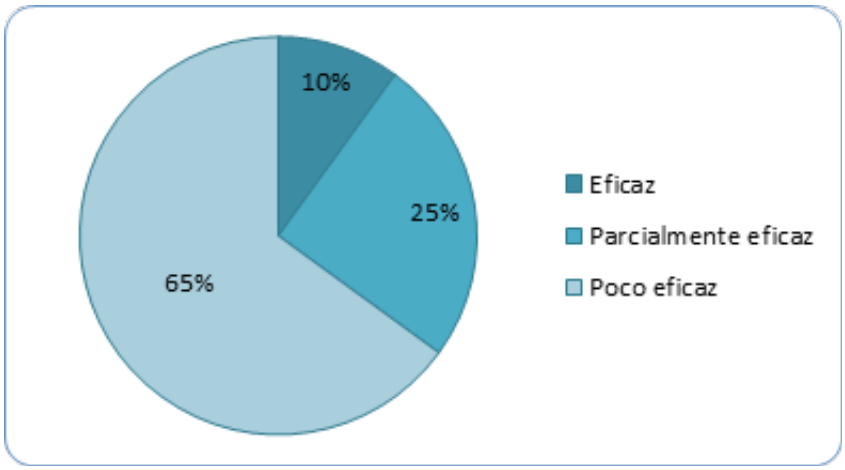


Fuente: Elaboración propia.

De los 89 encuestados, el 65% manifiesta que perciben la Política nacional de ciberseguridad como poco eficaz en la investigación y enjuiciamiento de delitos informáticos, el 25% considera que el sistema es parcialmente eficaz, debido a que carece de recursos y capacitación especializada y solo un 10% indica que el sistema es eficaz y está bien preparado para abordar casos de ciberdelincuencia.

Pregunta 2: ¿Cuáles son los principales desafíos que enfrenta la implementación de la Política Nacional de ciberseguridad?

Fig 2: Resultados de la pregunta 3 de la encuesta.

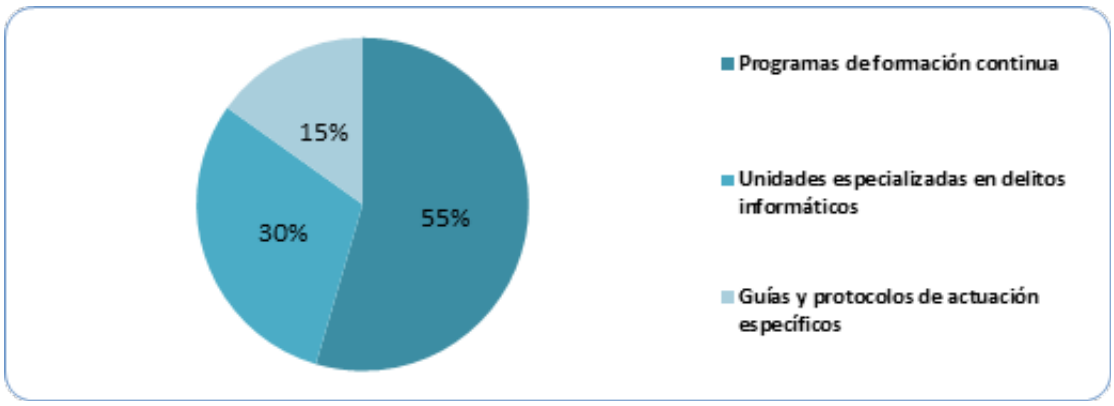


Fuente: Elaboración propia.

En esta pregunta el 30% de los encuestados identifican la falta de capacitación especializada en investigación forense digital por los operadores judiciales como el principal obstáculo, un 24% mencionó la falta de recursos tecnológicos, el 19% destaca la complejidad de la normativa vigente, el 21% la falta de coordinación interinstitucional como las barreras más significativas que afectan la eficacia de la implementación, y el 6% adujo otras causas no especificadas en el cuestionario, como la falta de concienciación sobre las amenazas cibernéticas y desactualización o inadecuada gestión de riesgos informáticos.

Pregunta 3: ¿Qué medidas considera necesarias para mejorar la eficacia de la Política Nacional de ciberseguridad?

Fig 3: Resultados de la pregunta 3 de la encuesta.



Fuente: Elaboración propia.

El 54% de los encuestados señalan la necesidad de implementar programas de formación continua para profesionales y funcionarios que ejerzan actividades vulnerables desde el punto de vista cibernético; un 30% sugirió la creación

de unidades especializadas en delitos informáticos dentro de la estructura judicial y el 15% restante propuso la elaboración de guías y protocolos de actuación específicos para facilitar la prevención, investigación y enjuiciamiento de casos de ciberdelincuencia.

Estos resultados reflejan la percepción de los participantes sobre la situación actual y las posibles estrategias para mejorar la respuesta del sistema judicial frente a los desafíos de la ciberseguridad en Ecuador.

Estos resultados indican que la falta de coordinación interinstitucional y la ausencia de protocolos claros para la prevención, investigación y persecución de delitos informáticos son algunos de los principales obstáculos que enfrenta el gobierno ecuatoriano. Asimismo, se identifica una brecha significativa en cuanto a la formación y capacitación de los profesionales cuya actividad está relacionada con la administración de justicia en casos de delitos de ciberseguridad. De forma mayoritaria el sistema es valorado como poco eficaz.

A partir de estos resultados, se realizan entrevistas para recabar información que permitiera elaborar recomendaciones para revertir las brechas identificadas. Los criterios de cada acción se muestran en la tabla 2.

Tabla 2: Recomendaciones para revertir las brechas identificadas.

Indicador	Acción	Descripción
Capacidad de respuesta	Creación de Unidades Especializadas	Establecer unidades especializadas en delitos informáticos dentro de la estructura judicial, con objetivos, principios y acciones específicas para fortalecer la ciberseguridad a nivel local, disponiendo de personal capacitado y recursos adecuados para investigar y enjuiciar casos relacionados con la ciberdelincuencia.
	Fortalecer la coordinación Interinstitucional	Promover la coordinación y colaboración entre instituciones gubernamentales, organismos encargados de la seguridad informática y el sistema judicial, como la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL) y el Comando Conjunto de las Fuerzas Armadas, que tienen responsabilidades en la protección y defensa de la infraestructura crítica y la seguridad cibernética con el fin de compartir información y recursos para combatir de manera efectiva los delitos cibernéticos.
	Elaboración de Guías de Procedimiento	Desarrollar guías y manuales de procedimiento que establezcan protocolos claros para la investigación y enjuiciamiento de delitos informáticos, facilitando el trabajo de los operadores judiciales y garantizando el debido proceso.
	Actualización de la Legislación	Continuar fortaleciendo el marco normativo en materia de ciberseguridad, mediante la revisión y actualización de leyes existentes y la promulgación de nuevas disposiciones que se adapten a los avances tecnológicos y las necesidades del país.
Educación en ciberseguridad	Programas de Formación Continua	Implementar programas de formación continua dirigidos a jueces, fiscales, abogados y funcionarios gubernamentales, con énfasis en aspectos jurídicos y técnicos de la ciberseguridad, para mejorar su capacidad para enfrentar los desafíos que presenta el entorno digital.
	Promoción de la confianza ciudadana	Crear programas de concientización y capacitación en ciberseguridad dirigidos a diversos sectores, con el propósito de sensibilizar a la población sobre los riesgos cibernéticos y proporcionar conocimientos y habilidades para la protección de la información

Fuente: Elaboración propia.

DISCUSIÓN

El Ecuador cuenta con una Estrategia Nacional de Ciberseguridad, documento que fija los lineamientos para la seguridad nacional en el ciberespacio y que cuenta con la participación de más de 170 actores de la sociedad civil, académicos, expertos en ciberseguridad, funciones del estado, sector privado y todas las instituciones que conforman el Comité Nacional de Ciberseguridad, organismo creado en el actual Gobierno y que aglutina los Ministerios de

Telecomunicaciones y de la Sociedad de la Información, Defensa Nacional, Gobierno, Interior, Relaciones Exteriores y Movilidad Humana, el Centro de Inteligencia Estratégica y la Secretaría General de la Administración Pública de la Presidencia.

La Política de Ciberseguridad de Ecuador que fue publicada mediante Registro Oficial No. 479, fue diseñada para proteger los activos digitales y la infraestructura crítica del país. Los bienes jurídicos del Estado en el espacio público digital pueden incluir información gubernamental, datos ciudadanos, sistemas críticos de infraestructura, y otros elementos esenciales para el funcionamiento del país, en este sentido, esta política busca abordar la ciberseguridad de manera integral, considerando la participación de diversos sectores, como el gobierno, el sector privado, la sociedad civil y otros actores relevantes.

Los principios rectores de la estrategia tienen por objetivo dirigir y orientar las actividades de todos los actores nacionales que trabajan en pro de la visión y el objetivo general de la Estrategia Nacional de Ciberseguridad. Su objetivo es proteger la soberanía del estado, la protección de la información de las instituciones y los ciudadanos, y garantizar que las acciones e iniciativas en materia de ciberseguridad sean holísticas, coherentes y estén en concordancia con los valores fundamentales compartidos (Ministerio de Telecomunicaciones y Sociedad de la Información, 2021).

Los resultados obtenidos a partir de la encuesta y las entrevistas realizadas en el presente estudio proporcionan una visión de las percepciones y experiencias de un grupo operadores judiciales y expertos en ciberseguridad de la ciudad de Babahoyo. Estas respuestas se han analizado en relación con la teoría existente en el campo de la ciberseguridad y la administración de justicia, contrastándose con investigaciones previas realizadas en otros países y en el propio Ecuador.

Uno de los resultados destacados del estudio es la identificación de la falta de coordinación interinstitucional como un obstáculo significativo en la administración de justicia en casos de delitos informáticos. Esta problemática se relaciona con la teoría que destaca la importancia de la colaboración entre diferentes entidades gubernamentales y organismos encargados de la seguridad informática para combatir eficazmente la ciberdelincuencia (Ferruzola et al., 2022).

Comparativamente, investigaciones realizadas en otros países de la región, como Colombia y México, también han señalado la necesidad de mejorar la coordinación interinstitucional para enfrentar los desafíos que presenta el cibercrimen (Ospina & Sanabria, 2020). Estos estudios resaltan la importancia de establecer mecanismos de cooperación y compartir información entre las autoridades competentes para investigar y enjuiciar adecuadamente los delitos informáticos.

Para la implementación efectiva de la Política Nacional de ciberseguridad en Ecuador, que influya directamente en el marco jurídico a fin de mejorar la capacidad de la administración de justicia para abordar y sancionar delitos cibernéticos, garantizando así la seguridad digital y la protección de información a los ciudadanos en el Ecuador, se destaca el artículo científico realizado por el autor (Parra, 2021).

Otro resultado relevante es la escasez de capacitación especializada del personal en materia de ciberseguridad. Esta carencia se refleja en la dificultad para investigar y enjuiciar casos relacionados con el ámbito digital de manera efectiva. Desde la teoría, se reconoce la importancia de la formación continua de los operadores judiciales para mantenerse actualizados sobre las nuevas tendencias y técnicas utilizadas por los delincuentes cibernéticos (Méndez, 2021). También se encuentra que los estudios se centran más en la ciberseguridad y las herramientas de protección que en educar en las ciberamenazas y concienciar (Beltrán et al., 2023).

Comparativamente, estudios realizados en países europeos como España y Alemania han resaltado la necesidad de programas de capacitación especializada en ciberseguridad para jueces y fiscales (Vidal, 2022). Estas investigaciones coinciden en que la falta de conocimiento técnico en el sistema judicial puede limitar la efectividad de la respuesta frente a los delitos informáticos y comprometer la protección de los derechos de los ciudadanos en el ciberespacio.

La formulación de una política nacional de ciberseguridad implica la consideración de diversas teorías que abordan la complejidad de los desafíos en el ciberespacio. La ciberseguridad se entiende no solo como una cuestión técnica, sino como un componente crítico de la seguridad nacional, la gobernanza global y la resiliencia de una nación en un mundo interconectado (Leiva, 2015).

En resumen, los resultados obtenidos en el presente estudio coinciden con la teoría y otras investigaciones en aspectos clave relacionados con la ciberseguridad y la administración de justicia. La falta de coordinación interinstitucional, la escasez de capacitación especializada y la necesidad de una legislación y procedimientos en consonancia con la realidad nacional, son desafíos comunes que deben abordarse para mejorar la respuesta gubernamental frente a los delitos informáticos en Ecuador. Estos hallazgos subrayan la importancia de implementar

medidas integrales y coordinadas que fortalezcan la capacidad del sistema judicial para enfrentar los desafíos que plantea el cibercrimen en el siglo XXI (Betancourt, 2017)

CONCLUSIONES

De forma mayoritaria el sistema es valorado como poco eficaz. La falta de coordinación entre instituciones gubernamentales y organismos encargados de la seguridad informática emerge como una barrera significativa en la eficacia de la lucha contra la ciberdelincuencia en Ecuador. Esta carencia dificulta la ejecución eficiente de acciones conjuntas para prevenir y perseguir delitos informáticos. La falta de capacitación especializada del personal gubernamental en el ámbito de la ciberseguridad revela una necesidad urgente de invertir en programas de formación continua y actualización profesional. Es preciso además crear programas de concientización y capacitación en ciberseguridad dirigidos a diversos sectores, con el propósito de sensibilizar a la población sobre los riesgos cibernéticos y proporcionar conocimientos y habilidades para la protección de la información.

Es fundamental contar con una legislación actualizada en consonancia con los actuales desafíos y riesgos informáticos que enfrenta el país. Además, se requiere la elaboración de guías de procedimiento que brinden orientación práctica a los operadores judiciales en el manejo de casos relacionados con la ciberdelincuencia. El país debe continuar fortaleciendo su política nacional de ciberseguridad, promoviendo la colaboración público- privada, la innovación y la adopción de buenas prácticas de seguridad cibernética que faciliten la protección de la información sensible y la mitigación de riesgos cibernéticos.

REFERENCIAS BIBLIOGRÁFICAS

Álvarez, T. (2022). Las garantías de los derechos fundamentales en y desde la red: El contexto español. ***Revista Chilena De Derecho Y Tecnología, 11***(1), 5-40. https://rchdt.uchile.cl/index.php/RCHDT/article/view/60197

Beltrán, A., Jiménez, M. G., & Sampayo, S. (2023). Métodos y efectos de la educación en ciberseguridad: una revisión sistemática. REC ***Revista Electrónica de Criminología, 7***. https://dialnet.unirioja.es/servlet/articulo?codigo=9295861

Betancourt, C. A. (2017). Ciberseguridad en los sistemas de información de las universidades. ***Dominio de las Ciencias, 3***(Extra 3), 200-217. https://dialnet.unirioja.es/servlet/articulo?codigo=6102849

Cando, M. R., & Medina, P. (2021). Prevención en ciberseguridad: enfocada a los procesos de infraestructura tecnológica. ***3C TIC Cuadernos de desarrollo aplicados a las TIC, 10***(1), 17-41. https://dialnet.unirioja.es/descarga/articulo/7888164.pdf

Caro, M. J. (2010). Alcance y ámbito de la seguridad nacional en el ciberespacio. Cuadernos de estrategia, 149(Ejemplar dedicado a: Ciberseguridad. ***Retos y amenazas a la seguridad nacional en el ciberespacio***, 47-82. https://dialnet.unirioja.es/servlet/articulo?codigo=3837251

Fernández, E. (2021). Desafíos jurídicos interdisciplinares de la ciberseguridad nacional: apuntes de lege ferenda. ***Anuario de la Facultad de Derecho. Universidad de Extremadura, 37***, 75-118. https://dehesa.unex.es/bitstream/10662/15424/1/2695-7728_37_75.pdf.

Ferruzola, E. C., Bermeo, O. X., & Arévalo, L. M. (2022). Analysis of centralized computer security systems through the alienvault ossim tool. ***Ecuadorian Science Journal***, ***6***(1), 23-31. https://journals.gdeon.org/index.php/esj/article/view/181/343

Leiva, E. (2015). Estrategias Nacionales de Ciberseguridad: Estudio Comparativo Basado en Enfoque Top-Down desde una Visión Global a una Visión Local. ***Revista Latinoamericana de Ingeniería de Software, 3***(4), 161-176. https://revistas.unla.edu.ar/software/article/view/775

Méndez, A. E. (2021). Análisis de políticas públicas de seguridad cibernética. Estudio del caso ecuatoriano. Polo del Conocimiento: ***Revista científico - profesional, 6***(3), 1229-1250. https://dialnet.unirioja.es/servlet/articulo?codigo=7926828

Ministerio de Telecomunicaciones y Sociedad de la Información. (2021). Estrategia Nacional de Ciberseguridad del Ecuador. Registro Oficial No. 479. https://asobanca.org.ec/wp-content/uploads/2022/08/ESTRATEGIA-NACIONAL-DE-CIBERSEGURIDAD-DEL-ECUADOR-2022481.pdf.

Moncayo, P. (2019). ***Herramientas jurídicas para garantizar la ciberseguridad del Estado. Análisis comparado de Colombia, Chile y Ecuador*** [Trabajo de titulación previo a la obtención del Título de Abogado de los Tribunales y Juzgados de la República, Universidad Central del Ecuador]. Quito. http://www.dspace.uce.edu.ec/handle/25000/19494

Ospina, M., & Sanabria, P. (2020). Desafíos nacionales frente a la ciberseguridad en el escenario global: un análisis para Colombia. ***Revista Criminalidad, 62***(2), 199-217. http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S1794-31082020000200199

Parra, R. (2021). Ecuador publica su política de ciberseguridad. DPL NEWS. https://dplnews.com/ecuador-publica-su-politica-de-ciberseguridad/

Sancho, C. (2017). Ciberseguridad. Presentación del dossier Cybersecurity. ***Revista Latinoamericana de Estudios De Seguridad, 20***, 8-15. https://revistas.flacsoandes.edu.ec/urvio/article/view/2859/2103

Vidal, M. D. (2022). Marco regulatorio de la ciberseguridad y ciberdefensa dentro de la sociedad de la información y el conocimiento: respuestas del Estado ecuatoriano en el período 2013-2022 [Maestría en Relaciones Internacionales, Universidad Andina Simón Bolívar]. http://hdl.handle.net/10644/9076