Preparación policial para responder al delito informático en Ecuador

Police preparedness to respond to cybercrime in Ecuador

Santiago Marcelo Tamayo Benavides [1], Mauricio Germán Delgado Montenegro [2]

INFORMACIÓN DEL ARTÍCULO

Fecha de recepción: 7 de Agosto de 2023.
Fecha de aceptación: 3 de Octubre de 2023.

[1] Doctor en Educación, Universidad Católica Andrés Bello. Docente-investigador, Fundación en Educación Integral para el Desarrollo Local (FEIDEL) - Ecuador.
E-mail: santiago.tamayo18627@gmail.com
Código ORCID:
https://orcid.org/0000-0002-8864-3515

[2] Doctorando en Educación, Universidad de Investigación e Innovación de México. Docente-investigador, Fundación en Educación Integral para el Desarrollo Local (FEIDEL) - Ecuador.
E-mail: feidel.educa58@hotmail.com
Código ORCID:
https://orcid.org/0009-0009-4109-6081

CITACIÓN: Tamayo Benavides, S.M., & Delgado Montenegro, M.G. (2023). Preparación policial para responder al delito informático en Ecuador. Podium, 44, 17–36.
doi:10.31095/podium.2023.44.2

ENLACE DOI:
http://dx.doi.org/10.31095/podium.2023.44.2

Resumen

El presente estudio pretende describir y explorar la preparación del personal policial ecuatoriano para responder al delito informático, para lo cual se aplicó una encuesta cuyos datos se utilizaron para analizar la frecuencia de participación en capacitaciones enfocadas a delitos informáticos; su nivel de confianza individual y organizacional para responder a este tipo de delito; y, la percepción sobre cómo mejorar su respuesta ante estos hechos. Se realizó una revisión de las investigaciones existentes sobre la complejidad de las investigaciones de delitos informáticos y la preparación policial para responder a los incidentes informáticos. Entre las conclusiones del estudio se sugiere que los policías ecuatorianos pueden beneficiarse de una mayor capacitación en habilidades básicas relacionadas con el delito informático.

Palabras Clave:
Formación policial, preparación policial, confianza individual, confianza institucional, delito informático, respuesta al delito informático.

Clasificación JEL: K240, I21.

Abstract

The present study aims to describe and explore the preparation of Ecuadorian police personnel to respond to cybercrime, for which a survey was applied whose data was used to analyze the frequency of participation in training focused on cybercrime, their level of individual and organizational confidence to respond to this type of crime; and the perception of how to improve their response to these facts. This is followed by a review of existing research on the complexity of cybercrime investigations and police preparedness to respond to cyber incidents. Among the study's conclusions, it is suggested that Ecuadorian police officers may benefit from more excellent training in basic skills related to cybercrime.

Keywords:
Police training, police preparedness, individual trust, institutional trust, cybercrime, response to cybercrime.

JEL Classification: K240, I21.

ISSN: 1390-5473 e-ISSN: 2588-0969

Introducción

El delito informático es toda actividad ilícita cometida mediante el uso de sistemas informáticos u otros dispositivos de comunicación o que tenga como finalidad el robo de información, apropiación del patrimonio económico o intelectual, el fraude financiero, la pornografía infantil, etc., es decir, desde el enfoque del derecho, los delitos informáticos se los puede catalogar como toda conducta típica, antijurídica y culposa que afecta la confidencialidad, integridad, patrimonio, acceso o disponibilidad de los datos de los sistemas informáticos y/o redes de telecomunicación (Chávez, 2021). El delito informático tiene una característica transnacional cuya naturaleza se constituye de grupos delictivos organizados radicados en una jurisdicción específica quienes cometen actos ilícitos en otra mientras que los bienes protegidos sustraídos terminan en una tercera (Sviatun y otros, 2021). Los daños que producen este tipo de delitos superan los costos financieros estimados y las víctimas en la mayoría de los casos experimentan problemas de salud física y mental como efectos consecuentes de estos actos ilícitos (Cross y otros, 2016).

En Ecuador, la población que tiene acceso a internet alcanza el 79,21% y cerca de 15,8 millones de ecuatorianos tienen cuentas en distintas redes sociales. Esta creciente navegación por el ciberespacio ha provisto de objetivos más visibles a los delincuentes, ha facilitado la identificación de potenciales víctimas y ha generado nuevas oportunidades para el delito, como consecuencia se ha identificado un incremento en la frecuencia de delitos informáticos. Según un informe estadístico de la Unidad de Ciberdelitos de la Policía Nacional del Ecuador, desde el año 2020 hasta el 6 de julio de 2022, se registraron 3.183 delitos informáticos (Redacción Seguridad, 2022).

Para Llumiquinga (2021), el Ecuador se encuentra en una etapa inicial de madurez en lo que respecta a la ciberseguridad, argumento que lo sustenta en dos estudios del estado de la ciberseguridad realizados por la Unión Internacional de las Telecomunicaciones (ITU), a esto debe sumarse que la percepción ciudadana se basa en lo que el ciudadano llega a conocer, es así que, las personas se enteran de los ataques informáticos, estafas u otros delitos informáticos que sufren instituciones, familiares, amigos o conocidos, pero no conocen el desenlace de estos hechos, por lo que las acciones que se adoptaron para contener, solventar, mitigar, denunciar o resolver estos problemas es incierta para la población, es así que el clamor de la población recae en la institución policial como entidad de primera respuesta ante los hechos delictivos.

La policía como primer respondedor debe tener el conocimiento básico que permita ayudar a las víctimas del delito informático durante el proceso de recepción de denuncias (Cross, 2020), además debe tener una comprensión de los conceptos básicos sobre el delito informático, de la normativa legal involucrada, de lo que implica el análisis forense digital, así también, debe contar

PODIUM No. 44, Diciembre 2023, pp. 17-36

ISSN: 1390-5473 e-ISSN: 2588-0969

con procedimientos o protocolos estandarizados de respuesta ante este tipo de delitos que permitan una actuación adecuada del policía y un manejo prolijo de los indicios.

El presente estudio pretende describir y explorar la preparación del personal policial ecuatoriano para responder al delito informático, para lo cual se aplicará una encuesta a una muestra representativa de servidores policiales, cuyos datos se utilizarán para analizar la frecuencia de participación en capacitaciones policiales enfocadas a delitos informáticos; los niveles de confianza individual y organizacional del personal policial para responder al delito informático; y, la percepción de los servidores policiales respecto a cómo mejorar esta respuesta.

Revisión de literatura

La complejidad de la investigación de delitos informáticos

La complejidad de la investigación de delitos informáticos nace desde la concepción del término, según Miró (2012) el delito informático incluye tipologías de conductas, y no tipos penales, por lo que indica que en los últimos años se ha venido sustituyendo esta denominación por la de cibercrimen y cibercriminalidad los cuales hacen referencia al término inglés *cybercrime*, concepto que permitiría abarcar la descripción de delincuencia en el ciberespacio. En Ecuador, la normativa legal vigente mantiene el término delito informático para referirse a tipos penales y para describir las tipologías de conducta. Por lo cual en el presente estudio se manejará el término de delito informático.

Según Miró (2013) el anonimato en la red y la transnacionalidad del delito complican los procesos judiciales debido a que pese que el delito informático se conoce que es cometido por alguien en concreto, en Internet solo se muestra una representación virtual del autor (la dirección IP) lo que conlleva que la policía deba investigar para atribuir la dirección IP a una persona física responsable de la acción delictiva, pero este trabajo es complejo en razón que el policía debe contar con la colaboración de las empresas proveedoras de servicios para determinar el sistema informático del cual se llevó a cabo el ataque. Después con la información proporcionada deberá investigar para dar con el titular de dicho sistema informático y, finalmente tendrá que concretar quién, de entre todos los usuarios del mismo sistema, ejecutó la acción. Además, la determinación judicial de las personas autoras del delito informático se complica por el carácter transnacional del delito, ya que el delito informático puede haber sido cometido en el extranjero y requerirá de la colaboración de otro Estado para poder llevar ante la justicia al delincuente, estas circunstancias pueden crear obstáculos para el trabajo policial ante la respuesta al delito informático.

En el marco legal internacional, la norma más relevante para establecer la jurisdicción de los delitos informáticos es el Convenio sobre la Ciberdelincuencia conocido también como “Convenio de

PODIUM No. 44, Diciembre 2023, pp. 17-36

ISSN: 1390-5473 e-ISSN: 2588-0969

Budapest", esta normativa proporciona un marco integral y coherente en contra del delito informático y la evidencia electrónica. Esta norma ha sido utilizada como guía para la elaboración de diferentes legislaciones a nivel local sobre el delito informático y también como marco de cooperación internacional entre los países miembros (Consejo de Europa [COE], 2022). Ecuador, pese a participar como observador en el Comité del Convenio sobre la Ciberdelincuencia, hasta la presente fecha no ha firmado ni ha ratificado este convenio internacional. Sin embargo, dentro de la normativa legal ecuatoriana se dispone de la Ley Orgánica de Protección de Datos Personales [LOPDP], el Código Orgánico Integral Penal (COIP, 2014) y normas conexas para combatir el delito informático. Pese a existir un marco legal que sanciona los delitos informáticos, los limitados recursos humanos y logísticos de la Unidad Nacional de Ciberdelito de la Policía Nacional del Ecuador complican su investigación. Al respecto Rappert y otros (2021) consideran que esta es una de las razones por la que los especialistas realizan su trabajo en razón de las prioridades de investigación de su organización.

Otros aspectos que complican la investigación del delito informático son: la inadecuada preservación de la escena del delito y el desconocimiento del manejo de la evidencia digital por parte del personal de primera respuesta, el cual debería ser consciente de que interactuar directamente con el contenido de los dispositivos incautados puede alterar la forma en que se almacenan estos datos y, por lo tanto, interrumpir la adquisición de evidencia digital. Por ejemplo, el acceso aparentemente inocuo a un dispositivo puede anular la información almacenada en la memoria de acceso aleatorio (brindando detalles sobre las acciones recientes del usuario), mientras que la alteración de los archivos almacenados en un dispositivo puede impedir la recuperación de los datos que se han eliminado, pero aún no se han sobrescrito (Holt y otros, 2019a, 2019b; Karie y otros, 2019).

La diversidad de dispositivos y sistemas operativos disponibles para consumidores, así como el acelerado desarrollo de las tecnologías informáticas estándar se transforman en elementos que complican la capacidad de los investigadores policiales para el uso de métodos científicamente fiables y reproducibles de análisis forense digital (Mason y Stanfield, 2017), el efecto de esto es que los organismos encargados de hacer cumplir la ley pueden estar utilizando herramientas forenses digitales de talla única (por ejemplo, "*The Forensic Toolkit*") para examinar el contenido de un dispositivo incautado que puede no cumplir con los estándares científicos necesarios para la admisibilidad en los tribunales (Casey, 2019).

Preparación de la policía para investigar el delito informático

El Estatuto Orgánico de Gestión Organizacional por Procesos de la Policía Nacional del Ecuador (Acuerdo Ministerial 080 de 2019) (Ministerio del

PODIUM No. 44, Diciembre 2023, pp. 17-36

ISSN: 1390-5473 e-ISSN: 2588-0969

Interior, 2019), contempla tres subsistemas de gestión, uno de los cuales es el subsistema de gestión general de investigación. El Director General de Investigaciones es el responsable de la gestión general de investigación, para lo cual tiene bajo su mando a diferentes Unidades y Direcciones Nacionales, entre las cuales se encuentra la Unidad Nacional de Ciberdelito. Al realizar un análisis comparativo de la estructura organizacional para responder al delito informático con otros países de la región, se puede identificar que en EEUU el 54% de las agencias de policía cuentan con una unidad especializada en delitos informáticos (Nowacki y Willits, 2019). En Chile, la Policía de Investigaciones cuenta con una unidad especializada para combatir el delito informático, esta se denomina unidad especializada de cibercrimen, la cual se conforma de brigadas investigadoras ubicadas en Santiago, Valparaíso y Concepción y tienen como misión el combate a este tipo de delito (Policía de Investigación [PDI], s.f.). Colombia cuenta por su parte con un departamento dentro de la unidad de investigación criminal de defensa para tratar este tipo de delitos.

El problema se da cuando la acción de la policía, como primer respondedor ante los eventos delictivos, no sea la adecuada a consecuencia de la falta de conocimientos básicos para responder al delito informático por parte de los agentes que llegan inicialmente a la escena del delito. Las diferentes policías clasifican a casi todas las categorías de delitos informáticos como de menor prioridad que los delitos "fuera de línea" o "tradicionales", excepto la distribución en línea de material de explotación infantil (Holt y otros, 2015). De manera similar, la policía generalmente tiene una comprensión pobre del abuso sexual basado en imágenes (es decir, compartir imágenes íntimas sin consentimiento) (Bond y Tyrrell, 2021) y otras formas de violencia sexual facilitada por la tecnología (Powell y Henry, 2018), tales creencias están vinculadas a la percepción de las víctimas como moralmente menos merecedoras de asistencia si comparten imágenes íntimas (Venema, 2019).

Estas percepciones del delito informático como comparativamente menos graves que los delitos fuera de línea se acrecientan por la falta de confianza de fuerzas del orden público en sus capacidades de investigación. Un estudio reciente del Reino Unido sugiere que el 61,5% de los agentes no se sienten preparados para investigar los delitos informáticos, lo que atribuyen principalmente a la falta de formación. Además, el 80,9% de los oficiales encuestados reportaron falta de confianza en las capacidades de sus organizaciones (Burruss y otros, 2019). Un estudio compuesto por grupos focales con dieciséis (16) policías británicos sugiere que la falta de confianza del policía se la puede atribuir a la creencia de que el delito informático es demasiado complejo; a las escasas o inadecuadas oportunidades de capacitación sobre delitos informáticos; y, a la confusión continua sobre la distinción entre la tipificación penal del "delito informático" y "delito fuera de línea" (Hadlington y otros, 2021). El estudio de Bossler y otros

PODIUM No. 44, Diciembre 2023, pp. 17-36

ISSN: 1390-5473 e-ISSN: 2588-0969

(2020), menciona que solo el 38,8% de los funcionarios del Reino Unido han recibido capacitación específica sobre delitos informáticos y solo el 42,4% de los funcionarios encuestados indicaron cierto grado de "preparación para responder al fraude en línea".

Con respecto a la formación policial, Casas y otros (2018) mencionan que la profesionalización es sin duda un factor clave para las policías del 2030 en América Latina, adicionalmente señalan que no existen evaluaciones externas rigurosas sobre la calidad de la educación policial, tampoco se encuentra análisis sobre la articulación de los procesos de formación con la incorporación policial y las condiciones laborales. Los autores resaltan que: "La profesión policial debe estar a la vanguardia de la formación de hombres y mujeres que en esencia prestarán un servicio público cuya razón de ser es la promoción de libertades, derechos y deberes." Por lo cual es indispensable una visión estratégica e innovadora para la preparación policial.

Un estudio de Choi y otros (2022) concluye que, para adaptarse al ritmo rápidamente cambiante del delito informático, es vital que la formación investigativa se adapte y desarrolle a través de la integración de VR, el estudio proporciona los hallazgos del estudio piloto de un novedoso entrenamiento de realidad virtual utilizado en tres áreas diferentes de investigaciones cibernéticas, que incluyen procedimientos de búsqueda e incautación. Según los hallazgos se identificó la importancia de integrar la formación en realidad virtual en los departamentos académicos y forenses, en especial para los miembros de cuerpos de seguridad ciudadana, lo cual comparte Ávalos (2021) al mencionar que, dada la particularidad del delito informático, es necesaria la constante capacitación de jueces, fiscales, peritos y la Policía Nacional en todo el territorio, por niveles y conforme con sus funciones.

Metodología

Este estudio involucra una investigación cuantitativa en la que se examinó la preparación del personal policial, del comando del servicio de la Policía Nacional para la Zona de Planificación No. 1 (Abarca las provincias de Esmeraldas, Carchi, Imbabura y Sucumbíos).

El objetivo de la investigación fue analizar la preparación del policía para responder al delito informático y el nivel de confianza individual y organizacional para una respuesta adecuada a este tipo de delito. Por lo cual, se plantearon cinco (5) preguntas de investigación:

P1: ¿Con qué frecuencia el personal policial asignado a la Zona No. 1 se enfrenta al delito informático?

P2: ¿Qué tan común es la capacitación en delitos informáticos entre el personal policial asignado a la Zona No. 1?

P3: ¿Qué confianza tiene el personal policial, asignado a la Zona No. 1, en sus habilidades individuales para responder al delito informático?

P4: ¿Qué confianza tiene el personal

PODIUM No. 44, Diciembre 2023, pp. 17-36

ISSN: 1390-5473 e-ISSN: 2588-0969

policial, asignado a la Zona No. 1, en las capacidades de su organización para responder al delito informático?

P5: ¿Qué recursos o habilidades cree el personal policial, asignado a la Zona No. 1, que son necesarios para mejorar las respuestas al delito informático?

Esta investigación utilizó un diseño no experimental exploratorio con aplicación de encuesta. Se aplicó un cuestionario a los policías asignados a la Zona de Planificación No. 1, 4149 hombres y 763 mujeres. De los cuales 1316 policías (1093 hombres y 223 mujeres) respondieron satisfactoriamente al cuestionario. Al no contar con el registro de la población y al encontrarse esta dispersa geográficamente, no se pudo aplicar el muestreo probabilístico, por lo que se optó por aplicar un muestreo no probabilístico, el cual no incluye ningún tipo de muestreo aleatorio, por lo que se ha seleccionado sujetos accesibles y disponibles para formar parte de la muestra (McMillan y Schumacher, 2005). Como la participación estuvo influenciada por efectos de autoselección, los resultados no son completamente representativos de la población y no deben generalizarse sin observar las características de la muestra como se indica en la Tabla 1.

Para López y otros (2019), la validez viene a ser el grado en el cual un instrumento cuantifica lo que debe medir, conduciendo a conclusiones válidas, en este caso la preparación policial para responder al delito informático. El instrumento de la encuesta es adaptado de estudios previos de Wilson y otros (2022), por lo que se sometió a revisión de su contenido, pertinencia, ambigüedad y redacción, posterior de lo cual se analizó la confiabilidad realizando un ensayo piloto. El valor α= ,923 se obtuvo al aplicar la prueba a todo el test, es decir existe una alta consistencia interna de los ítems dentro de la escala. Con respecto a la validez del constructo se efectuó el análisis factorial exploratorio aplicando la prueba KMO obteniendo un valor excelente de ajuste del modelo y significancia estadística en el valor en la prueba de esfericidad de Bartlett (ver Tabla 2).

Tabla 2.
Prueba de KMO y Bartlett

Medida Kaiser-Meyer- Olkin de adecuación de muestreo		,938
Prueba de esfericidad de Bartlett	Aprox. Chi-cuadrado	14394,453
	gl	406
	Sig.	,000

Fuente: Elaboración propia.

Tabla 1.
Características servidores policiales muestreados de la Zona de Planificación Nº 1

Característica	Categoría	Total
Subsistema de Gestión (*n*=1316)	Preventivo	1139 (86 ,6%)
	Investigativo	177 (13 ,4%)
Función que desempeña (*n*=1316)	Operativo	1074 (81 ,6%)
	Administrativo	242 (18 ,4%)
Sexo (*n*=1316)	Masculino	1093 (83 ,1%)
	Femenino	223 (16 ,9%)

Fuente: Elaboración propia.

PODIUM No. 44, Diciembre 2023, pp. 17-36

ISSN: 1390-5473 e-ISSN: 2588-0969

La muestra no ponderada se analizó mediante programa SPSS™, versión 25. Se realizó análisis descriptivos para explorar el acuerdo general del personal policial según los conjuntos de elementos. Posteriormente, se realizaron una serie de análisis bivariados (Pruebas Chi-cuadrado de Pearson) para determinar si existían diferencias significativas en la confianza individual y organizacional según cuatro variables independientes categóricas (Subsistema de gestión, función, educación y sexo), con la V de Cramer como medida del tamaño del efecto.

Resultados

Encuentros previos con el delito informático

Se exploró los encuentros del personal con incidentes de delitos informáticos y su capacitación en delitos informáticos. En relación a los encuentros del personal con incidentes de delitos informáticos los resultados sugieren que el 65,4% de encuestados (n=861) nunca ha respondido a un incidente de delincuencia informática. Sin embargo, una minoría de encuestados (n=272, 20,7%) informa que su último encuentro fue dentro de los últimos 12 meses, mientras que el 13.9% de encuestados (n=183) indicó que la última vez que respondió a un delito informático fue hace más de un año. Un resumen de las respuestas se puede encontrar en la Tabla 3.

Analizamos estos patrones según el subsistema de gestión, la función y el sexo de los encuestados. Los resultados sugieren que el personal del subsistema preventivo informó encuentros más recientes con incidentes de delitos informáticos que el personal del subsistema investigativo. La exposición a incidentes de delitos informáticos tiene

Tabla 3.
Prevalencia comparativa de la exposición más reciente a incidentes de delitos informáticos

	Subsistema de gestión		Función		Sexo		Total
	P.	I.	O.	A.	H.	M.	
Dentro de la última semana	35 (3,1%)	4 (2,3%)	32 (3,0%)	7 (2,9%)	26 (2,4%)	13 (5,8%)	39 (3,0%)
Dentro de las últimas seis semanas	61 (5,4%)	1 (0,6%)	53 (4,9%)	9 (3,7%)	56 (5,1%)	6 (2,7%)	62 (4,7%)
Dentro de los últimos seis meses	85 (7,5%)	2 (1,1%)	73 (6,8%)	14 (5,8%)	76 (7,0%)	11 (4,9%)	87 (6,6%)
Dentro del último año	73 (6,4%)	11 (6,2%)	67 (6,2%)	17 (7,0%)	69 (6,3%)	15 (6,7%)	84 (6,4%)
Hace más de un año	151 (13,3%)	32 (18,1%)	156 (14,5%)	27 (11,2%)	161 (14,7%)	22 (9,9%)	183 (13,9%)
Nunca	734 (64,4%)	127 (71,8%)	693 (64,5%)	168 (69,4%)	705 (64,5%)	156 (70,0%)	861 (65,4%)

Nota: P=Preventivo, I=Investigativo, O=Operativo, A=Administrativo, H=Hombre, M=Mujer.
Fuente: Elaboración propia.

PODIUM No. 44, Diciembre 2023, pp. 17-36

ISSN: 1390-5473 e-ISSN: 2588-0969

una relación débil con el subsistema de gestión, χ^2=20,919, $\rho < 0,05$, V=,126. Según la función de los encuestados no existen diferencias significativas, así como tampoco existe una relación entre las variables χ^2=3,457, $\rho > 0,05$, V=,051. Con relación a la variable sexo no se evidencia una diferencia significante, sin embargo, existe una relación débil entre la variable sexo y la exposición más reciente a un incidente de delito informático, χ^2=14,957, $\rho < 0,05$, V=,107.

Al respecto de su capacitación en delitos informáticos se les consultó si han tenido entrenamiento en algunos campos relacionados este tipo de delito, un 73.3% de los encuestados indicaron que no se incluyo en su proceso de formación policial algún módulo sobre el uso de Internet o el delito informático (n = 964), mientras que solo un 26.7% señala que se incluyó en su proceso de formación policial algún módulo sobre el uso de Internet o el delito informático (n = 352).

Entrenamiento para responder el delito informático

Solo el 20,6% (n=271) de los encuestados afirma haber completado una formación sobre sensibilización general sobre el delito informático (ver Tabla 4). A pesar de informar encuentros menos frecuentes con incidentes de delitos cibernéticos, los encuestados del subsistema de investigación informaron datos significativamente más altos de conciencia general en delitos informáticos (n=59, 33,3%) en comparación con los encuestados del subsistema preventivo (n=212, 18,6%). Con respecto a formas de capacitación más especializadas no hubo diferencias significativas entre los dos subsistemas.

El personal investigativo tenía más probabilidad de haber completado una

Tabla 4.
Prevalencia del entrenamiento en ciberdelincuencia según el subsistema de gestión

¿Ha recibido entrenamiento en alguno de los siguientes temas?	Total		Preventivo		Investigativo				
	No	Sí	No	Sí	No	Sí	χ^2	ρ	V
Conciencia general sobre el delito informático	1045	271	927	212	118	59	20,301	,000	,124
	79,4%	20,6%	81,4%	18,6%	66,7%	33,3%			
Orientación de denunciantes de victimización por delitos informáticos, para realizar una denuncia formal ante fiscalía	1029	287	902	237	127	50	4,974	,026	,061
	78,2%	21,8%	79,2%	20,8%	71,8%	28,2%			
Toma de informe inicial sobre un caso de delitos informáticos de una víctima o denunciante	1162	154	1012	127	150	27	2,497	,114	,044
	88,3%	11,7%	88,8%	11,2%	84,7%	15,3%			
Recopilar y/o preservar evidencia digital cuando una persona busca denunciar la victimización por un delito informático	1176	140	1029	110	147	30	8,568	,003	,081
	89,4%	10,6%	90,3%	9,7%	83,1%	16,9%			
Dirigir a los denunciantes a otras agencias gubernamentales o no gubernamentales que puedan ayudar, en los casos en que no se pueda identificar un delito imputable	1155	161	1012	127	143	34	9,266	,002	,084
	87,8%	12,2%	88,8%	11,2%	80,8%	19,2%			
Uso de código abierto o inteligencia disponible públicamente	1214	102	1061	78	153	24	9,650	,002	,086
	92,2%	7,8%	93,2%	6,8%	86,4%	13,6%			
Técnicas de investigación digital	1200	116	1052	87	148	29	14,579	,000	,105
	91,2%	8,8%	92,4%	7,6%	83,6%	16,4%			
Legislación nacional pertinente o relevante para delitos informáticos	1216	100	1065	74	151	26	14,643	,000	,105
	92,4%	7,6%	93,5%	6,5%	85,3%	14,7%			
Legislación estatal o territorial pertinente o relevante al delito informático	1224	92	1067	72	157	20	5,839	,016	,067
	93,0%	7,0%	93,7%	6,3%	88,7%	11,3%			

Fuente: Elaboración propia.

PODIUM No. 44, Diciembre 2023, pp. 17-36

ISSN: 1390-5473 e-ISSN: 2588-0969

capacitación general sobre concientización sobre delitos informático en comparación con los policías preventivos, así como capacitación específica sobre cómo recopilar y preservar evidencia digital, técnicas de investigación digital y legislación pertinente. Más allá de estas diferencias, el número de personal preventivo que informa haber completado capacitación en áreas más especializadas (por ejemplo, cómo dirigir al público para que denuncie un delito informático; cómo registrar una denuncia inicial de delito informático) fue notablemente bajo. Por ejemplo, menos del 30% de los policías preventivos habían recibido capacitación sobre cómo orientar a las víctimas de delitos informáticos para denunciar en fiscalía y menos del 10% habían recibido entrenamiento sobre la preservación de evidencia digital cuando se encontraron inicialmente con un caso de victimización.

Niveles de confianza individual

Más de la mitad de los encuestados indicaron que tenían al menos "algo de confianza" en sus capacidades para responder al delito informático (n=836, 63.6%) (ver Tabla 5). Utilizando una variante consolidada de tres puntos de este ítem, no se observa diferencias significativas en los niveles de confianza individual según el subsistema de gestión de los encuestados. Menos del 40% de encuestados del subsistema preventivo informaron tener al menos "confianza" en su propia capacidad para responder al delito cibernético (n=410, 36%) de manera similar con los encuestados del subsistema de investigativo (n=63, 35,6%), χ^2=,45, $\rho > 0,05$, V=,006. Los policías operativos (n=390, 36,3%) no tuvieron altas diferencias en comparación con los policías administrativos (n=83, 34,3%), χ^2=,736, $\rho > 0,05$, V=,024. Los encuestados según su sexo presentaron una leve diferencia, las mujeres encuestadas tuvieron mayor probabilidad de informar tener al mayor "confianza" en su propia capacidad para responder al delito cibernético (n=97, 43,5%) en comparación con los encuestados hombres (n=376, 34,4%), χ^2=8,221, $\rho < 0,05$, V=,079.

Niveles de confianza en la organización

En comparación con los niveles de confianza individual, el personal policial presentó una leve diferencia a favor de la confianza en las capacidades de su institución para responder al delito

Tabla 5.
Distribución de respuestas al ítem que mide el nivel de confianza individual

	Nada confiado		Con desconfianza		Algo desconfiado		Confiado		Muy confiado	
Preventivo	233	20,5%	183	16,1%	313	27,5%	317	27,8%	93	8,2%
Investigativo	32	18,1%	32	18,1%	50	28,2%	51	28,8%	12	6,8%
Total	265	20,1%	215	16,3%	363	27,6%	368	28%	105	8%

Fuente: Elaboración propia.

PODIUM No. 44, Diciembre 2023, pp. 17-36

ISSN: 1390-5473 e-ISSN: 2588-0969

informático de manera efectiva. Los resultados indican que menos de la mitad de los encuestados estaban "nada confiados" o "con desconfianza" en las capacidades de su institución (n=441, 33.5%). Por el contrario, una porción mayor de los encuestados mencionó que tenían "confianza" o "mucha confianza" en las capacidades de su institución (n = 525, 39.9%) (ver Tabla 6).

Se observó una leve diferencia al correlacionar el nivel de confianza en la organización según si un encuestado había recibido en su proceso de formación policial algún módulo sobre el uso de Internet o el delito informático. Los encuestados que tuvieron en su proceso de formación policial algún módulo sobre el uso de Internet o el delito informático indicaron tuvieron más probabilidad de reportar confianza en su organización (n=175, 49,7%) en comparación con los que no tuvieron en su proceso de formación policial algún módulo sobre el uso de Internet o el delito informático (n=350, 36,3%), χ^2=20,178, $\rho < 0,05$, V=,124.

Además de una medida general de confianza en la organización, también preguntamos a los encuestados una serie

Tabla 6.
Distribución de respuestas al ítem que mide el nivel de confianza en la organización

	Nada confiado		Con desconfianza		Algo desconfiado		Confiado		Muy confiado	
Preventivo	217	19,1%	160	14,0%	306	26,9%	377	33,1%	79	6,9%
Investigativo	32	18,1%	32	18,1%	44	24,9%	59	33,3%	10	5,6%
Total	249	18,9%	192	14,6%	350	26,6%	436	33,1%	89	6,8%

Fuente: Elaboración propia.

Tabla 7.
Respuestas a ítems que miden aspectos de la respuesta de la organización al delito informático

	Nada confiado	**Algo confiado**	**Confiado**
Toma el delito informático tan en serio como los delitos cara a cara o físicos	430 32,7%	352 26,7%	534 40,6%
Financiamiento y recursos adecuados para abordar los delitos informáticos	484 36,8%	413 31,4%	419 31,8%
Eficaz en el apoyo a las víctimas del delito informático	423 32,1%	377 28,6%	516 39,2%
Efectivo en la detección de perpetradores de delitos informáticos	437 33,2%	383 29,1%	496 37,7%
Eficaz para acusar a los perpetradores de delitos informáticos	421 32,0%	399 30,3%	496 37,7%
Eficaz en la prevención del delito informático	402 30,5%	380 28,9%	534 40,6%
Efectivo en la interrupción del delito informático	423 32,1%	399 30,3%	494 37,5%

Fuente: Elaboración propia.

PODIUM No. 44, Diciembre 2023, pp. 17-36

ISSN: 1390-5473 e-ISSN: 2588-0969

de sub-preguntas que miden la confianza en capacidades específicas (tres niveles). Al igual que con la confianza general, la mayoría de los encuestados (más del 50%) indicaron "Nada confiado" o "Algo desconfiado" en las capacidades de su organización en las siete sub-preguntas (ver Tabla 7).

No hubo diferencias significativas entre los encuestados de los subsistemas preventivo e investigativo en estos elementos. Sin embargo, hubo diferencias observables según el sexo de los encuestados (ver Tabla 8). Las encuestadas tuvieron más probabilidad de confiar de que su organización estuviera tomando el delito informático tan en serio como los delitos cara a cara (n=100, 44,8%) en comparación con los encuestados (n=434, 39,7%). χ^2=12,184, $\rho < 0,05$, V=,096. También se observa que los hombres encuestados tienen más probabilidades de carecer de confianza en las capacidades de su organización para acusar a los ciberdelincuentes (n=373, 34,1%) en comparación con sus contrapartes mujeres (n=48, 21,5%), χ^2= 16,743, $\rho < 0,05$, V=,113. Finalmente, se examina la relación entre los niveles de confianza individual y organizacional. Los datos completos de la tabulación cruzada se pueden encontrar en la Tabla 9. Específicamente, los encuestados

Tabla 8.
Respuestas a ítems que miden aspectos de la respuesta de la organización al delito informático según el sexo de los encuestados

	Hombre			Mujer					
	Nada confiado	Algo confiado	Confiado	Nada confiado	Algo confiado	Confiado	χ^2	ρ	v
Toma el delito informático tan en serio como los delitos cara a cara o físicos	379 34,7%	280 25,6%	434 39,7%	51 22,9%	72 32,3%	100 44,8%	12,184	,002	,096
Financiamiento y recursos adecuados para abordar los delitos informáticos	428 39,2%	341 31,2%	324 29,6%	56 25,1%	72 32,3%	95 42,6%	19,773	,000	,123
Eficaz en el apoyo a las víctimas del delito informático	375 34,3%	310 28,4%	408 37,3%	48 21,5%	67 30,0%	108 48,4%	15,423	,000	,108
Efectivo en la detección de perpetradores de delitos informáticos	388 35,5%	312 28,5%	393 36,0%	49 22,0%	71 31,8%	103 46,2%	16,039	,000	,110
Eficaz para acusar a los perpetradores de delitos informáticos	373 34,1%	331 30,3%	389 35,6%	48 21,5%	68 30,5%	107 48,0%	16,743	,000	,113
Eficaz en la prevención del delito informático	355 32,5%	314 28,7%	424 38,8%	47 21,1%	66 29,6%	110 49,3%	12,998	,002	,099
Efectivo en la interrupción del delito informático	372 34,0%	328 30,0%	393 36,0%	51 22,9%	71 31,8%	101 45,3%	11,687	,003	,094

Fuente: Elaboración propia.

Tabla 9.
Comparación de los niveles de confianza individual y organizacional de los encuestados

Confianza individual	Ninguna	Algo	Con confianza	Total
Confianza institucional				
Ninguna	327 (68,10%)	68 (18,80%)	46 (9,80%)	441 (96,70%)
Algo	79 (16,50%)	207 (57,00%)	64 (13,50%)	350 (87,00%)
Con confianza	74 (15,40%)	88 (24,20%)	363 (76,70%)	525 (116,30%)
Total	**480 (100%)**	**363 (100%)**	**473 (100%)**	**1316 (100%)**

Fuente: Elaboración propia.

PODIUM No. 44, Diciembre 2023, pp. 17-36

ISSN: 1390-5473 e-ISSN: 2588-0969

tenían más probabilidades de tener al menos algo de confianza en las respuestas de su organización al delito informático si también reportaban confianza en sus capacidades individuales, χ^2=16,743, ρ < 0,05, V=,113.

Importancia percibida para mejorar las investigaciones de delitos informáticos

El conjunto final de elementos midió las percepciones de los encuestados sobre qué habilidades o recursos ayudarían a

Tabla 10.
Respuestas a ítems que miden la importancia percibida para mejorar las investigaciones de delitos informáticos

	Nada importante	**No tan importante**	**Algo importante**	**Importante**	**Muy importante**
Mejor educación para el ciudadano sobre cómo mantenerse seguro en línea	36 2,70%	29 2,20%	154 11,70%	444 33,70%	653 49,60%
Mayores recursos para herramientas y tecnologías forenses digitales	44 3,30%	18 1,40%	140 10,60%	440 33,40%	674 51,20%
Sanciones más severas para los ciberdelincuentes	41 3,10%	25 1,90%	116 8,80%	406 30,90%	728 55,30%
Cooperación con las empresas víctimas para mejorar la denuncia de delitos	39 3,00%	22 1,70%	132 10,00%	460 35,00%	663 50,40%
Trabajar con empresas de Internet (por ejemplo, Google, Facebook, Twitter) para "vigilar" Internet	38 2,90%	28 2,10%	147 11,20%	460 35,00%	643 48,90%
Mayor inversión en unidades especializadas en delitos de alta tecnología	41 3,10%	24 1,80%	125 9,50%	434 33,00%	692 52,60%
Aumento de la financiación para la formación de policías en ciberdelincuencia	39 3,00%	26 2,00%	122 9,30%	439 33,40%	690 52,40%
Mayor desarrollo de las capacidades nacionales para hacer frente a la ciberdelincuencia .	37 2,80%	20 1,50%	125 9,50%	442 33,60%	692 52,60%
Mayor desarrollo de capacidades en todo el estado o territorio para abordar el delito informático	36 2,70%	16 1,20%	134 10,20%	457 34,70%	673 51,10%
Mayor desarrollo de las capacidades locales para hacer frente a la ciberdelincuencia	38 2,90%	23 1,70%	123 9,30%	469 35,60%	663 50,40%
Legislación más clara contra los delitos informáticos para aumentar el éxito del enjuiciamiento y las investigaciones	38 2,90%	20 1,50%	135 10,30%	428 32,50%	695 52,80%

Fuente: Elaboración propia.

PODIUM No. 44, Diciembre 2023, pp. 17-36

ISSN: 1390-5473 e-ISSN: 2588-0969

mejorar las respuestas al delito informático. Un resumen completo de los resultados se puede encontrar en la Tabla 10. Los encuestados estaban a favor de las medidas propuestas en diversos grados. La tendencia claramente se enfoca a que todos los aspectos consultados eran "muy importantes" o "importantes" para los encuestados. No hubo diferencias significativas según el subsistema de gestión, la función o el sexo del encuestado.

Conclusiones

El reporte de datos proporciona evidencia sobre la preparación del personal de la policía ecuatoriana para responder de manera efectiva a los incidentes de ciberdelincuencia. Los datos sugieren que, si bien los oficiales del subsistema preventivo tenían más probabilidades de encontrar incidentes de delitos informáticos, era menos probable que reporten haber completado los tipos de capacitación necesarios para los "primeros respondedores" en las escenas del delito informático. Estos servidores policiales también tenían menos probabilidades de sentirse seguros de sus capacidades personales para responder de manera efectiva a los incidentes de ciberdelincuencia. En general, los datos revelan algunas capacidades y déficits de confianza entre el personal encuestado que tienen consecuencias en el mundo real para las víctimas del delito informático (Cross, 2020), pero también resaltan el deseo de mejores recursos y mayores oportunidades de capacitación dentro de la institución policial.

Los hallazgos sugieren que la policía ecuatoriana casi no enfrenta delitos informáticos en la actualidad. Específicamente, el 64,5% de los policías del subsistema preventivo reportaron nunca haber respondido a un incidente de ciberdelincuencia y menos del 15% de los encuestados reportó haber completado algún tipo de capacitación sobre delitos informáticos, lo que responde la primera y segunda pregunta de investigación. La proporción de encuestados que informa haber completado una capacitación general relacionada con el delito informático no supera las tasas de Reino Unido, donde el 38,8 % de los oficiales de servicio general informaron haber completado dicha capacitación (Bossler y otros 2020), sin embargo, los datos obtenidos se asimilan a los obtenidos en el estudio de Ávila y Rincón (2023) quienes concluyen que el 22,3% de los patrulleros encuestados indicaron no tener conocimiento sobre cómo realizar denuncias de delitos informáticos o ante qué entidad acudir. Esto sugiere tentativamente que el personal policial de la Subzona de Planificación No. 1 tienen personal comparativamente menos preparado para responder a incidentes de delitos informáticos. Solo el 11,7% de los encuestados indica haber recibido capacitación sobre como tomar un informe inicial sobre un caso de delitos informáticos de una víctima o denunciante y solo el 10,6% menciona haber recibido instrucción básica sobre la preservación de evidencia digital. Ambas habilidades son esenciales para los "primeros respondedores" de incidentes de ciberdelincuencia y no requieren

PODIUM No. 44, Diciembre 2023, pp. 17-36

ISSN: 1390-5473 e-ISSN: 2588-0969

conocimientos sofisticados de análisis forense digital.

Específicamente, la investigación identifica la necesidad de una capacitación personalizada de los policías del subsistema preventivo sobre cómo recibir y derivar a las víctimas de un delito informático y habilidades básicas para la gestión digital de la escena del crimen (cómo preservar la evidencia electrónica en el momento en que se reporta un incidente). Aunque solo el 8,8% de todos los encuestados había recibido formación especializada en técnicas de investigación digital, dichas habilidades son comparativamente más complejas e implican un conocimiento más detallado de la ciencia forense digital. En general, el personal de la policía ecuatoriana no ha recibido una capacitación adecuada referente al delito informático, por lo que la institución se beneficiaría capacitando y preparando a su personal en estas áreas y temáticas.

Los datos sugieren que existe una pequeña mayoría del personal encuestado informa cierta medida de desconfianza en sus capacidades individuales. Con respecto a la función que desempeñan, los encuestados presentan la misma tendencia leve hacia la desconfianza en sus capacidades individuales y no se evidencia una diferencia significativa. Esto ayuda a responder la tercera pregunta de investigación. Se puede afirmar que en este aspecto los datos son consistentes con investigaciones realizadas en la policía europea, las cuales examinaron la preparación de los agentes del orden público en el Reino Unido, donde los oficiales de servicio general tenían una confianza “moderada” para responder a incidentes de ciberdelincuencia (por ejemplo, Bossler y otros, 2020), de manera similar, el estudio de Guerrero (2022) concluye que el 55,7% de los encuestados indicó que hubo un nivel medio de capacidades institucionales en las investigaciones por delitos informáticos.

Es importante destacar que el análisis respalda la relación entre tener una capacitación específica en delitos informáticos y niveles más altos de confianza individual para responder a incidentes de delitos informáticos (por ejemplo, Burruss y otros, 2019). Por lo tanto, es probable que las tasas más bajas de capacitación entre los policías del subsistema preventivo sean un factor que contribuya al déficit de confianza observado. Respecto a la variable educación, existe una ligera diferencia entre los encuestados que tienen un nivel técnico, tecnológico o de tercer nivel, quienes presentan una leve tendencia a una mayor confianza individual, mientras que el personal sin educación superior (bachilleres) y quienes tienen una educación de cuarto nivel, tuvieron una leve tendencia a la desconfianza de sus capacidades individuales para responder al delito informático.

Estas relaciones deben interpretarse de manera crítica, en lugar de simplemente tomarse al pie de la letra, ya que la investigación sugiere que el desconocimiento o la alta especialización podrían presentar una cierta desconfianza en las capacidades individuales para

PODIUM No. 44, Diciembre 2023, pp. 17-36

ISSN: 1390-5473 e-ISSN: 2588-0969

responder el delito informático, mientras que el personal técnico, tecnológico y de tercer nivel podrían estar tendiendo a sobrestimar sus habilidades en ciberseguridad (por ejemplo, Martens y otros, 2019). Esto podría sugerir que la relación entre la capacitación, la educación y la confianza autoinformada no se traduce en diferencias reales en las habilidades. Sería necesario realizar más investigaciones para evaluar dicha relación.

Por el contrario, los datos de este estudio sugieren que el personal policial generalmente confía en las capacidades de su institución para responder al delito informático. Esto ayuda a responder la cuarta pregunta de investigación. Las pocas investigaciones al respecto señalan que los especialistas en delitos informáticos se sienten sin recursos y mal equipados para lidiar con un número cada vez mayor de referencias de casos de delitos cibernéticos. La frecuencia de delitos informáticos, podría ser un factor para que en la policía ecuatoriana confíe en la capacidad de su institución, ya que no han podido experimentar una alta frecuencia de incidentes informáticos, a lo que no sabrían cómo responder según los datos obtenidos en capacitación, por lo que debería realizarse un análisis e investigación diferentes para determinar si la institución policial ecuatoriana tiene la capacidad para responder al delito informático adecuadamente. Curiosamente, los datos de esta investigación también sugieren que el personal que se siente personalmente inseguro al responder a incidentes de delitos cibernéticos era más propenso a expresar desconfianza en las capacidades de su institución, lo que destaca el nexo entre los niveles de confianza de un individuo y las políticas y procedimientos de la organización (por ejemplo, Bossler y otros, 2020).

Los datos también brindan información sobre las opiniones del personal policial sobre las posibles soluciones a este déficit de confianza, y los oficiales generalmente apoyan una variedad de iniciativas en diversos grados. Esto ayuda a responder la quinta pregunta de investigación. Principalmente, los encuestados tuvieron una preferencia similar por cada uno de los aspectos consultados, lo que puede sugerir una necesidad que no es percibida aún por los encuestados. Sin embargo, los resultados también sugieren que el personal reconoce la importancia de cada uno de estos componentes. En general, los encuestados confiaban modestamente en sus propias capacidades, pero tendrían una mayor confianza en su institución.

Los resultados sugieren que el personal policial anhela más recursos organizacionales y oportunidades de capacitación. Como tal, existe una posible necesidad de más recursos por parte de la Policía de la Zona de Planificación No. 1 para mejorar las capacidades organizativas de respuesta al delito informático, incluyendo la mejora de las habilidades del personal con conocimientos básicos sobre cómo gestionar las escenas del crimen digital, la preservación de la evidencia digital y los procedimientos para recibir y derivar a las víctimas de delitos informáticos. Otra alternativa sería la creación de un

PODIUM No. 44, Diciembre 2023, pp. 17-36

ISSN: 1390-5473 e-ISSN: 2588-0969

centro o equipo de respuesta a incidentes de seguridad (CSIRT por las siglas de Computer Security Incident Response Team) que permita la gestión de incidentes informáticos en materia de seguridad pública y ciudadana con policías altamente especializado en delitos informáticos.

Los resultados reflejan la percepción de la muestra autoseleccionada del personal policial de la Zona de Planificación No. 1, por lo tanto, las experiencias del personal de otras zonas de planificación pueden diferir de la examinada actualmente. Esta es una limitación importante a reconocer, dada la influencia de las experiencias personales y las políticas organizacionales en las perspectivas de los policías sobre el delito informático. La investigación futura podría evaluar la calidad de los módulos de capacitación sobre delitos informáticos existentes y desentrañar las razones por las que existe una discrepancia entre los niveles de confianza individuales e institucionales con mayor detalle. Sería útil tener datos más específicos sobre las habilidades que les faltan a los policías. Esto ayudaría a garantizar que los programas de capacitación aborden brechas sustanciales en el conocimiento. Por lo que se recomienda para estudios futuros explorar las habilidades que requieren los policías preventivos o de primera respuesta para atender el delito informático.

Contribución de autores

S.M.T.B: Idea, revisión de literatura, diseño de la investigación, metodología, análisis de datos, y redacción del artículo.

M.G.D.M: Diseño de la investigación, validación del modelo teórico, análisis de datos, y redacción del artículo.

Referencias

Ávalos, Z. (2021). Necesidad de especialización para combatir la ciberdelincuencia. *Revista Institucional de la Academia de la Magistratura,* (15), 43-62.

Ávila, F. y Rincón, P. (2023). Inclusión de la formación en prevención y atención de delitos informáticos en la educación policial. *Revista Educación, 47*(2). http://doi.org/10.15517/revedu.v47i2.53905

Bond, E., y Tyrrell, K. (2021). Understanding revenge pornography: a national survey of police officers and staff in England and Wales. *Journal of Interpersonal Violence, 36*(5–6), 2166–2181. https://doi.org/10.1177/0886260518760011

Bossler, A. M., Holt, T. J., Cross, C., y Burruss, G. W. (2020). Policing fraud in England and Wales: examining constables' and sergeants' online fraud preparedness. *Security Journal, 33*(2), 311–328. https://doi.org/10.1057/s41284-019-00187-5

Burruss, G., Howell, C. J., Bossler, A., y Holt, T. J. (2019). Self-perceptions of English and Welsh constables and sergeants preparedness for online crime. *Policing (Bradford, England), 43*(1), 105–119. https://doi.org/10.1108/PIJPSM-08-2019-0142

Casas, K., González, P., y Mesías, L. (2018). La transformación policial para el 2030 en América Latina. En Informe del programa de estado de derecho (Ed.), *Peter D. Bell y el Banco Interamericano de Desarrollo*. Banco Interamericano de Desarrollo.

Casey, E. (2019). The chequered past and risky future of digital forensics. *Australian Journal of Forensic Sciences, 51*(6), 649–664. https://doi.org/10.1080/00450618.2018.1554090

PODIUM No. 44, Diciembre 2023, pp. 17-36

ISSN: 1390-5473 e-ISSN: 2588-0969

Chávez, F. (2021). Ciberdelitos: una primera aproximación y proyección institucional. *Perfil criminológico*, 55-61. https://www.fiscalia.gob.ec/pdf/politica-criminal/Ciberdelitos-Perfil-Criminologico.pdf

Choi, Lee, H., Park, G., y Han, C. (2022). Virtual Reality Program in Cybercrime Investigation: A Pilot Study Examining Search and Seizure of Digital Evidence Practice. *Cyberpsychology, Behavior and Social Networking, 25*(1), 43–50. https://doi.org/10.1089/cyber.2020.0894

Código Orgánico Integral Penal [COIP]. (2014). Suplemento del Registro Oficial Nro. 180, 10 de febrero de 2014 (Ecuador). https://www.asambleanacional.gob.ec/es/system/files/document.pdf

Consejo de Europa [COE]. (2022, 21 de junio). *Adhesión al Convenio de Budapest sobre la Ciberdelincuencia: Beneficios*. https://rm.coe.int/cyber-buda-benefits-junio2022-es-final/1680a6f9f4#:~:text=Chile%2C%20Colombia%2C%20Costa%20Rica%2C,%2C%20Portugal%2C%20Ruman%C3%ADa%20y%20Suecia.

Cross, C., Richards, K., y Smith R. (2016). The reporting experiences and support needs of vicitms of online fraud. *Trends y Issues in Crime and Criminal Justice*, (518), 1-14.

Cross, C. (2020). 'Oh we can't actually do anything about that': The problematic nature of jurisdiction for online fraud victims. *Criminology & Criminal Justice, 20*(3), 358–375. https://doi.org/10.1177/1748895819835910

Guerrero, R. (2022). *Capacidades Institucionales y su incidencia en la carga procesal en las investigaciones por ciberdelincuencia, distrito fiscal de Lima Centro, 2022*. [Tesis de maestría, Universidad César Vallejo]. https://repositorio.ucv.edu.pe/handle/20.500.12692/97838

Hadlington, L., Lumsden, K., Black, A., y Ferra, F. (2021). A qualitative exploration of police officers' experiences, challenges, and perceptions of cybercrime. *Policing (Bradford, England), 15*(1), 34–43. https://doi.org/10.1093/police/pay090

Holt, T. J., Burruss, G. W., y Bossler, A. M. (2015). *Policing cybercrime and cyberterror*. Carolina Academic Press.

Holt, T. J., Burruss, G. W., y Bossler, A. M. (2019a). An examination of English and Welsh constables' perceptions of the seriousness and frequency of online incidents. *Policing and Society, 29*(8), 906–921. https://doi.org/10.1080/10439463.2018.1450409

Holt, T. J., Clevenger, S., y Navarro, J. (2019b). Exploring digital evidence recognition among officers and troopers in a sample of a state police force. *Policing (Bradford, England), 43*(1), 91–103. https://doi.org/10.1108/PIJPSM-07-2019-0119

Karie, N. M., Kebande, V. R., Venter, H. S., y Choo, K.-K. R. (2019). On the importance of standardizing the process of generating digital forensics reports. *Forensic Science International: Report, 1*. https://doi.org/10.1016/j.fsir.2019. 100008

Llumiquinga, G. (2021). Estrategia Nacional de Ciberseguridad en el Ecuador. *Perfil Criminológico*, 48-53. https://www.fiscalia.gob.ec/pdf/politica-criminal/Ciberdelitos-Perfil-Criminologico.pdf

López, R., Avello, R., Palmero, D., Sánchez, S. y Quintana, M. (2019). Validación de instrumentos como garantía de la credibilidad en las investigaciones científicas. *Revista Cubana de Medicina Militar, 48*(1), 441-450.

Martens, M., De Wolf, R., y De Marez, L. (2019). Investigating and comparing the predictors of the intention towards taking security measures against malware, scams and cybercrime in general. *Computers in Human Behavior, 92*, 139–150. https://doi.org/10.1016/j.chb.2018.11.002

Mason, S., y Stanfield, A. (2017). Authenticating electronic evidence. En S. Mason, y D. Seng (Eds.), *Electronic evidence* (pp. 193–260). University of London Press.

McMillan, J., y Schumacher, S. (2005).

PODIUM No. 44, Diciembre 2023, pp. 17-36

ISSN: 1390-5473 e-ISSN: 2588-0969

Investigación educativa (5ta ed.). Pearson Educación.

Ministerio del Interior. (mayo 14, 2019). Acuerdo Ministerial 0080 de 2019. *Estatuto Orgánico de Gestión Organizacional por Procesos de la Policía Nacional*. Registro Oficial Edición Especial 911. https://www.policia.gob.ec/wp-content/uploads/downloads/2020/09/ESTATUTO-ORGANICO-DE-LA-POLICIA-NACIONAL.pdf

Miró, F. (2012). *El Cibercrimen fenomenología y criminología de la delincuencia en el ciberespacio*. Marcial Pons.

Miró, F. (2013). *Delincuencia asociada al uso de las TIC.* [Recurso de aprendizaje textual]. Fundación Universitat Oberta de Catalunya (FUOC).

Nowacki, J., y Willits, D. (2019). An organizational approach to understanding police response to cybercrime. *Policing (Bradford, England), 43*(1), 63–76. https://doi.org/10.1108/PIJPSM-07-2019-0117

Policía de Investigaciones [PDI]. (s.f.). *Brigadas Investigadoras del Cibercrimen*. https://www.pdichile.cl/institución/unidades/cibercrimen

Powell, A., y Henry, N. (2018). Policing technology-facilitated sexual violence against adult victims: police and service sector perspectives. *Policing and Society, 28*(3), 291–307. https://doi.org/10.1080/10439463.2016.1154964

Rappert, B., Wheat, H., y Wilson-Kovacs, D. (2021). Rationing bytes: managing demand for digital forensic examinations. *Policing and Society, 31*(1), 52–65. https://doi.org/10.1080/10439463.2020.1788026

Redacción Seguridad. (25 de julio de 2022). 3 183 delitos informáticos se han registrado en el Ecuador, desde el 2020. *El Comercio*. https://www.elcomercio.com/actualidad/seguridad/3183-delitos-informaticos-se-han-registrado-en-el-ecuador-desde-el-2020.html

Sviatun, O., Goncharuk, O., Roman, C., Kuzmenko, O., y Kozych, I. (2021). Combating cybercrime: economic and legal aspects. *WSEAS Transactions On Environment And Development, 18*, 751-762.

Venema, R. M. (2019). Making judgments: how blame mediates the influence of rape myth acceptance in police response to sexual assault. *Journal of Interpersonal Violence, 34*(13), 2697–2722. https://doi.org/10.1177/0886260516662437

Wilson, M., Cross, C., Holt, T., y Powell, A. (2022). Police preparedness to respond to cybercrime in Australia: An analysis of individual and organizational capabilities. *Journal of Criminology, 55*(4), 468–494. https://doi.org/10.1177/26338076221123080

PODIUM No. 44, Diciembre 2023, pp. 17-36

ISSN: 1390-5473 e-ISSN: 2588-0969