INVESTIGACIÓN INTEGRAL Y ESPECIALIZADA EN LA PREVENCIÓN Y SANCIÓN DE LA CIBERDELINCUENCIA

COMPREHENSIVE AND SPECIALIZED RESEARCH IN THE PREVENTION AND PUNISHMENT OF CYBERCRIME

Leónidas Santiago Carhuas Huamán[1a]
Nilton César Velazco Lévano[2b]

Fecha de recepción : 05/08/2024
Fecha de aprobación : 20/12/2024
DOI : https://doi.org/10.26495/khxn0z14

Resumen

La investigación tuvo como objetivo describir el enfoque integral y especializado en la prevención y sanción de la ciberdelincuencia. Se trató de un estudio descriptivo con revisión sistemática, considerando 15 artículos científicos de acceso abierto publicados en los últimos cinco años, en función de las variables analizadas. El enfoque fue cualitativo, empleando una guía de revisión sistemática como instrumento. Los resultados muestran que el 70% de los autores señala que las investigaciones incluyen denuncias de robos masivos de información. Sin embargo, la mayoría de los países carece de una normativa específica y sólida para sancionar estos delitos, además de herramientas especializadas para su investigación, lo que vulnera los derechos de los ciudadanos. Por otro lado, el 30% de los autores indica que, en países desarrollados, los ciberdelitos afectan principalmente a grandes empresas, mientras que los ciudadanos son víctimas de forma más esporádica debido a hackers más selectivos. Aunque estos países cuentan con normativas robustas y emplean medidas preventivas como la codificación extrema de datos, enfrentan dificultades para lidiar con bandas criminales extranjeras. Se concluye que la investigación integral y especializada para prevenir y sancionar la ciberdelincuencia es insuficiente. Los vacíos legales y normativos, junto con la falta de tecnología y recursos adecuados, limitan la capacidad de los sistemas de justicia para abordar de manera efectiva este tipo de delitos.

Palabras clave: *Investigación integral, prevención de delitos, ciberdelincuencia, sanción de delitos.*

Abstract

The aim of the research was to describe the comprehensive and specialized approach to the prevention and punishment of cybercrime. It was a descriptive study with a systematic review, considering 15 open access scientific articles published in the last five years, based on the variables analyzed. The approach was qualitative, using a systematic review guide as an instrument. The results show that 70% of the authors indicate that the investigations include reports of massive theft of information. However, most countries lack specific and solid regulations to punish these crimes, as well as specialized tools for their investigation, which violates the rights of citizens. On the other hand, 30% of the authors indicate that, in developed countries, cybercrimes mainly affect large companies, while citizens are victims more sporadically due to more selective hackers. Although these countries have robust regulations and use preventive measures such as extreme data encryption, they face difficulties in dealing with foreign criminal gangs. It is concluded that comprehensive and specialized research to prevent and punish cybercrime is insufficient. Legal and regulatory gaps, together with the lack of adequate technology and resources, limit the capacity of justice systems to effectively address this type of crime.

Keywords: *Comprehensive investigation, crime prevention, cybercrime, criminal punishment.*

[1]*Ministerio Público – Ucayali - Perú*
[2]*Universidad César Vallejo – Tarapoto - Perú*
[a]*Maestro en Derecho penal y Procesal Penal, Orcid: https://orcid.org/0000-0002-7349-3622, Email: lcar54015@gmail.com*
[b]*Doctor en Derecho y Ciencia Política, Orcid: https://orcid.org/0000-0001-8809-9022, Email: niltonsj@hotmail.com*

1. Introducción

Actualmente, la tecnología y globalización han desarrollado aspectos tecnológicos en línea para realizar diferentes actividades, desde transacciones, ventas, acciones gubernamentales y otros en línea, almacenando una gran cantidad de base de datos de las personas e instituciones, esto ha sido también una oportunidad para el aprovechamiento de la delincuencia, buscando la forma de aprovechar el internet y la conexión digital económica para realizar robos cibernéticos. Es así como las empresas han reportado casi 500 millones de ataques de ransomware, y 3400 millones de phishing como las modalidades comunes de robos cibernéticos en todo el mundo, generando un costo de cerca casi cinco millones de dólares, incluyendo pérdida de datos en el sector salud con un costo de casi 10 millones en el año 2022 (Kolesnokov, 2024).

Así mismo, en la parte financiera mundial, ha reportado caso de robos cibernéticos en casi 3 millones de dólares, fuera de los costos de seguridad que afectó a miles de clientes glabales (Nataluccci, et.al., 2024). Esto demuestra que la ciberdelincuencia se ha incrementado, afectando a clientes, usuarios e instituciones, donde las instancias judiciales aún no han podido intervenir eficientemente para combatirla, más en países menos desarrollados que carecen de tecnologías para la prevención y sanción respectivamente.

En esa medida, concerniente a Perú, la ciberdelincuencia ha ganado terreno, pese a contar con leyes que protegen a las instituciones y usuarios de las redes, que se disfraza de diferentes modalidades para buscar información personal y luego proceden a usar dichos datos personales específicos para sus propósitos delincuenciales. Ante ello, se tiene la Resolución Legislativa N°3013 ratificada por DS N° 010, que luego se promulga el 2013 mediante ley N° 30096 y modficada el 2014 por la ley N°30171 y modificada por el DL N°1591 legislando los delitos de manera específica mediante tipificación para la creación de la fiscalía especializada de ciberdelincuencia con ley N°1503 MP-FN (Vinelli, 2021). Dicha normativa, ayuda a la investigación y sanción de la ciberdelincuencia en el país.

Por otra parte, en el país, la normativa existente es muy buena, sin embargo, carece de eficiencia en su aplicación, debido a las altas responsabilidades sin recursos para aplicarla, generando diversos inconvenientes a las fiscalías especializadas en las diferentes dependencias del país. Esto ha generado un crecimiento delincuencial cibernética del 2013 al 2020 de 12 mil denuncias a un incremento total del 70% en los últimos años, siendo las más comunes las estafas y fraudes informáticos en el sistema financiero con cerca de 22 mil denuncias (Defensoría del Pueblo, 2023). Esto evidencia el incremento de delitos informáticos específicos en el país, unos más fuertes que otros, ac arreándole un costo al estado para investigar y sancionar estos delitos, que muchas veces quedan impunes.

Además, la división de delitos informáticos de Alta Tecnología -DIVIANDAT, a pesar de tener todas las funciones, carece de herramientas y equipos pertinentes, y sin presupuesto para realizar investigaciones y prevenir el ciberdelito en el país; por otro lado, esta ausente el uso de tecnología forense especializada para poder analizar imágenes, videos u otros elementos de prueba o de tecnología para prevenir y sancionar ciberdelitos (Carbajal, 2022).

En esa medida, el trabajo es importante porque busca revisión bibliográfica de estudios que ayuden a comprender la normativa de la investigación integral y especializada en la prevención y sanción de ciberdelitos, que será de gran utilidad a la comunidad científica en función a los aspectos teóricos que servirán para trabajos similares. Metodológicamente, el trabajo será importante por la metodología descriptiva simple que servirán para otros trabajos en adelante.

¿Cómo es la investigación integral y especializada en la prevención y sanción de la ciberdelincuencia? Y las preguntas específicas: ¿Cómo se realiza la investigación integral y especializada de la ciberdelincuencia? ¿Cómo se da la prevención y sanción de la ciberdelincuencia?

Así mismo, se tiene el objetivo general como: Describir la investigación integral y especializada en la prevención y sanción de la ciberdelincuencia: Con objetivos específicos como: Conocer cómo se

realiza la investigación integral y especializada en la ciberdelincuencia. Y describir el proceso de prevención y sanción de la ciberdelincuencia.

Aspectos teóricos

En relación a los trabajos previos, se tiene los internacionales como Castillo (2023), en su estudio realizado en Colombia, con la finalidad de realizar un análisis de la ciberseguridad en el sector educación de fuerza aeroespacial, estudiando en su estudio mixto. Tuvo como resultados que existe una alta adaptación tecnológica, con ciberactividad, con uso contante de internet y redes; ello a conllevado que el vandalismo en robo de datos se ha incrementado. Además, hay mucha exposición de información de datos, que son extraídos por personas inescrupulosas para aprovecharse y tener al asecho a sus víctimas, donde los delincuentes usan métodos sofisticados para apoderase de la información, métodos y tecnología que carece la policía para prevenir y sancionar estos casos. La ciberdelincuencia no solo afecta el ciberespacio, si no tiene graves consecuencias en el espacio físico, para ello la prevención y ciberseguridad de información es necesaria.

Por tanto, Díaz, et al. (2023), en su trabajo realizado en Colombia, en la que buscó analizar la aproximación al ciberdelincuente desde la perspectiva del control social y la aplicación de normativa; Dentro de los resultados se tuvo que él ciberdelincuente tiene algunas características narcisistas, que busca apoderarse de información de datos para chantajear a sus víctimas con su modo operandi de despreocupación y modernización de formas y medios para delinquir en 37%. En Colombia los expertos de la Dirección de Investigación Criminal e INTERPOL, obteniendo que las tecnologías de información y comunicaciones forman parte del ciberespacio pero que tienen efecto en la parte física de las personas considerado en un análisis matricial. Además, se tuvo en cuenta en contraste con las teorías del control social se han abordado actos ciber delincuenciales de manera formal, donde el Estado cumple con la normativa, sin embrago carece de herramientas y presupuesto para hacer cumplir las leyes implementado acciones para investigar y prevenir ciberdelitos que atormentan a la población.

Además, López (2022), en su trabajo realizado en España, donde buscó analizar el alcance de los fines de la pena en el fenómeno criminal de ciberdelincuencia. Dentro de los resultados se pudo observar que en el caso de delitos cibernéticos se atribuyen a las teorías absolutas o retributivas, en la que los delitos de esta índole su culpabilidad en superior y a arrea grandes consecuencias, sin embrago las sanciones son débiles en el marco penal, viéndose reducido el delito a una contribución para las víctimas con justificaciones que avalan prácticamente al que comete el delito. Además, referente a la finalidad preventiva general del delito de la ciberdelincuencia fue menor al espacio físico tradicional en 32%, en la que a pesar de existir un alista larga de crímenes similares no hay espacios de alta tecnología de persecución e identificación de identidad de este tipo de delincuentes en 041%, rebajando la eficacia de los procesos y castigos, que siguen intimidando a sus víctimas. En conclusión, no se han desarrollado procesos específicos y eficientes para prevenir la ciberdelincuencia.

Seguidamente, Ospina y Sanabría (2020), en su trabajo realizado en Colombia, buscando analizar los desafíos nacionales frente a la ciberseguridad en Colombia. Dentro de los resultados obtuvo que existen muchas denuncias cibernéticas en apoderamiento de datos en 34% y robos de las cuentas de los usuarios de bancos en 38%, donde la población presenta mucha vulnerabilidad ante este tipo de delitos, A pesar de existir legislación general, no hay legislación sólida en materia de seguridad o protección de información, hay carencia de barreras para acceso a información por parte de terceros o codificación de información extrema. En conclusión, no se ha implementado softwares especializados a la política para poder detectar y prevenir delitos cibernéticos, con tecnología deficiente para sancionar estos delitos que cada día van incrementándose en la ciudad. Tampoco hay mapas de riesgos donde se dan más estas amenazas usando información del ciudadano.

También, Mayer y Óliver (2020), en su trabajo realizado en Chile, buscando analizar el delito del fraude informático o ciberdelito, enfatizando sus conceptos y limitaciones. Los resultados analizados mostraron que, a pesar de la cantidad de teorías en materia de fraude informático o ciberdelitos, aún no

se han aplicado teorías específicas en materia legal para prevenir este tipo de casos. En la mayoría de casos estos delitos quedan impunes, dado que hay etapas como de ejecución imperfecta o actos preparatorios de fraude por formar parte de categoría de hackeo o sabotaje informático, por la que la normativa debe ser tajante y específica para castigar este tipo de conductas como delitos informáticos, en ese sentido las teorías y las normativas deben ampliarse regulando tres requisitos copulativos verificando la conducta manipulativa, la provocación del delito y el fin de lucro de la acción en perjuicio del patrimonio institucional o personal.

De igual manera, Padalka (2022), en su trabajo realizado en Ucrania con el objetivo de analizar el apoyo criminalístico forense y técnico de la investigación de la ciberdelincuencia. En Ucrania abunda el ciber espionaje con ciberataques al Estado, a las empresas y ciudadanos, apropiándose de datos, y dinero de cuentas bancarias, esto se da por agencias de otros países, siendo delitos con fines de lucro para estas organizaciones que atemorizan a Ucrania, con sistemas modernos que son detectados para la prevención respectiva. Hay respuesta inmediata a estas ciber amenazas, con investigaciones policiales inteligentes forenses. Además, en la parte normativa es muy eficiente para sancionar internamente en el país este tipo de delitos, sin embrago es complicado sancionar bandas criminales externas, por ello el Estado se prepara para la preparación de protección de datos e información delicada y evitar este tipo de problemas.

También está Pérez y Rodríguez, en su trabajo realizado en el Ecuador, buscando analizar las implicancias sociales de los delitos cibernéticos. Dentro de los resultados se obtuvo que existe pocos estudios de investigaciones sociales interdisciplinarios. Además, se encontró que se han tomado falsas creencias sobre la seguridad en línea, desvirtuando la interpretación de manera individual o en conjunto, aduciendo que las víctimas de robos cibernéticos son responsables de brindar información específica o delicada para el delincuente, y el segundo son personas anónimas que no se pueden investigar ni sancionar, para ello se debe realizar investigaciones explicativas que demuestren la normativa con el mundo real, con tecnología que identifique al victimario. Concluyendo que existen muchos hechos de delitos cibernéticos que se trasladan del espacio físico al ciberespacio, sin embargo, no son sancionados por la falta de recursos de los administradores de justicia y la cantidad de delitos cometidos y el escaso apoyo social.

A su vez, se tiene estudios previos nacionales como Ávila (2024), en su trabajo realizado en Perú, buscando analizar el tipo penal de fraude cibernético en la legislación peruana. Resultando que, la tipificación del delito ciber delincuencial está en el marco del convenio Budapest dentro de la normativa internacional, por ello, la ciberdelincuencia no tiene una normativa específica si no general y amplia. Concluyendo que a pesar que la ciberdelincuencia trae consigo consecuencias diversas que muchas veces el propio sujeto que con engaños hace que el delincuente acceda a datos confiables, que luego sacan provecho de la misma, sin muchas veces ser detectados o castigados legalmente.

Así mismo, se tienen antecedentes nacionales como: Arapa, et al. (2024), en su trabajo realizado en Puno, con el fin de describir los delitos informáticos y analizar las causas y consecuencias del incremento de delitos cibernéticos en Puno. Los resultados mostraron que hubo un incremento considerable de la ciberdelincuencia; además se reportó información irregular de los delitos denunciados con desinformación, escasa herramientas en tecnología de la policía y falta de conciencia para la prevención por parte del gobierno y las empresas, con una precaria ciberseguridad, las víctimas son generalmente ciudadanos de entre 27 a 59 años de edad en 55%. Concluyendo que la información excesiva de las personas en las redes, o la exposición de datos de cuentas bancarias, hace que haya una gran tendencia a convertirse en víctimas, y muchas veces los delitos quedan impunes por carecer de aplicación de normativa firme o no contar con tecnología de punta para identificar los responsables.

También está Estrada (2024), en su trabajo realizado en Huánuco, buscando realizar un análisis de la impunidad de delitos informáticos como una problemática de poco interés las los administradores de justicia. En la legislación peruana se observa mucha impunidad de delitos informáticos, identificando factores para no llegar a una sanción a este tipo de delincuencia, dentro de ellos figura la no individualización de este tipo de delito, conllevando al archivo de los procesos. Al darse este tipo de

casos, el sujeto en cuestión no es considerado como hecho constituido de manera individual y el proceso legal de investigación exige una plena individualización, por ende, no se puede seguir con el hecho de manera formal; además existen vacíos legales que dejan impunes los casos. Concluyendo que, la delincuencia está ganado al ordenamiento jurídico, con defiende tecnología de delitos para investigación de manera integral y sancionar estos delitos que dañan a la sociedad.

En cuanto a Gomero y Sánchez (2024), en su trabajo realizado en Lima, buscando describir la realidad de ciberseguridad en los servicios de apoyo a los médicos. Los resultados mostraron los establecimientos de salud, el 80% tuvo planes respondiendo inmediatamente a este tipo de delitos, garantizando buenas acciones de ataques cibernéticos, buscando proteger la información y los datos, colocándolos con copias los datos vulnerables y críticos en diferentes establecimientos de salud; además siempre realizaban visitas inopinadas y otros operativos con softwares de seguridad para resguardar los datos, de esa manera prevenir robos o ciberataques delincuenciales. Concluyendo que existe gestión informática reactiva ante los ataques delincuenciales, dado que el país carece de reglas y herramientas normativas y presupuestales para castigar este tipo de delitos sin que haya perjuicios críticos en el espacio físico, por ello la importancia de la ciberseguridad debido a la transformación digital en que vivimos.

Además, está Ruíz y Solís (2024), en su trabajo realizado en Lima, con el fin de estudiar el fraude cibernético en modo phishing en la división de investigación de delitos de alta tecnología. Los resultados mostraron que los robos cibernéticos se dan mediante envío de correos a las víctimas para apoderase de información oportuna para extorsionarlos en 37%, o bajo la modalidad de enlaces masivos con virus en 49%, o suplantan páginas de entidades financieras en 29%, donde solicitan datos específicos y puntuales de los clientes y los códigos CCI, teléfonos y claves token para apoderarse de dinero de las cuentas bancarias. Además, siempre estos delitos quedan impunes por la no detección ni prevención por parte de la policía, perdiendo sus ahorros de trabajo los ciudadanos, faltando a su derecho de vivir en un espacio de paz y desarrollo. Concluyendo que los ciudadanos deben cuidar su información y corroborar enlaces sospechosos que soliciten datos personales o confidenciales, evitar compartir información que pueda generar infiltraciones en sus datos que serán perjudiciales.

Además, está Ramírez, et al. (2022), realizada en Perú, buscando analizar la conciencia del ciberdelito en estudiantes del Perú. Resultando que hubo cuatro tipos de ciberdelitos como phishing, spamming y otra forma de sotfware antivirus de acoso en las redes; además, existen causas de relaciones de parejas entre facultades como causa del bullying en las redes, sin embrago la mayoría de facultados no tienen conciencia del ciberdelito, usando la discriminación, la mofa y cualquier otra excusa para apoderarse de datos cibernéticamente, con una influencia de 0.89, 0.75, y 074 entre todos los delitos. Concluyendo que existe relación directa entre el ciberdelito y la conciencia de los estudiantes, pero se necesitan mayares herramientas para castigar legalmente este tipo de delitos, aunque parezcan no muy fuertes como la ciberdelincuencia de organizaciones criminales.

Marco teórico sobre las variables

Según el Ministerio de salud pública y bienestar social, la investigación integral de la ciberdelincuencia como es la teoría del delito, que ayuda a los procesos para la organización, identificando medios probatorios para demostrar la ocurrencia del delito (Carrera, et. Al., 2020). También se conoce el delito como como un elemento fundamental para iniciar una investigación con el trabajo policial y de un fiscal de una zona determinada, buscando disminuir la delincuencia y tener mejores resultados con el castigo del que delinque (Leyva, 2021). Además, el delito se da cuando una persona transgrede las reglas o normas que perjudican a un tercero, en el caso del delito cibernético se da cuando usan información o datos de una persona sin su consentimiento para sacar una ventaja económica o de otra índole que perjudica económicamente o socialmente a los ciudadanos o empresas.

Brevemente, se tiene la teoría de la pena que indica que el Estado es el padre generador del Estado de derecho, y los administradores de justicia emiten las normas legales junto con los legisladores, controlando el sistema penal para administrar justicia y el control de la sociedad, por ello, los

individuos que causen infracciones a la ley deben ser castigados dentro del sistema penal y la constitución política del Perú (Entralgo, et. al., 2014). También está la teoría absoluta de la pena indica que el Estado a través de la justica tutela los derechos de los ciudadanos de una determinada circunscripción, donde la comisión de delitos se encarga de investigar y perseguir e imponer pena correspondiente a los infractores.

Además, está la teoría de la garantía procesal, ligada a los derechos fundamentales indicadas en la constitución política, amparando a los ciudadanos para pedir al sistema judicial medidas de protección o búsquedas de justicia (Polyakov, 2019). Las mismas buscan respetar los derechos humanos, donde los administradores de justicia deben impartir de manera imparcial la misma respaldando y espetando los derechos de los ciudadanos en general y sin excepción.

Seguidamente, se tiene las teorías del internet de las cosas, conocida como Internet of Things (IoT), haciendo referencia que hoy en día las personas, los negocios e instituciones están interconectados con el internet, con dispositivos como teléfonos, máquinas, plataformas digitales, redes sociales y otros; interconectados para intercambiar información oportuna para compras y ventas. Ello hace que el mundo interactúe de manera física y virtual mediante la información y la tecnología. También, el internet de las cosas, está atribuido a los equipos, objetos u otras herramientas interconectadas gracias al internet, para detectar, recopilar, e intercambiar información en redes sociales de manera directa o por Wifi, las mismas necesitan de configuraciones (Jiménez y Medina, 2023). Este, genera un ecosistema que, por un lado, permite al usuario interactuar con los objetos físicos presentes en el establecimiento, y por el otro, otorga a las empresas la capacidad de capturar datos importantes relacionados con el comportamiento de compra, para así obtener un conocimiento profundo de las necesidades del cliente.

En particular, destacan los siguientes principios como: el principio de objetividad que se refiere al actuar de la fiscalía o los entes rectores de justicia a buscar la verdad, para ello debe buscar medos probatorios contundentes y la posibilidad de defensa al imputado, adecuando los procesos para una determinación correcta (Poaquiza, et.al., 2020). Es decir, el principio de objetividad debe ser contundentes, con pruebas claras para culpar al imputado para evitar cometer injusticias. También, está el principio de investigación previa, pues se debe ajustar a la objetividad y al cumplimiento de las normas legales, sin pasar por encima de los derechos de los ciudadanos, con los tiempos correspondientes para los descargos del imputado y determinar un veredicto justo (Ortíz y López, 2024).

En esa medida, la investigación integral especializada dentro del Código Procesal Penal, debe tener condiciones para juzgar al imputado con igualdad de oportunidades, elementos y herramientas, con oportunidad de descargo y pena justa (Meléndez, et. al., 2021). Muchas veces no se cumplen estos principios ya sea negándole la oportunidad de defensa a los imputados y los alegatos infundados de muchas personas que la final resultan inocentes. En sí, la investigación integral y especializada. Es un tipo de investigación que participan diversos actores involucrados de manera especializada y específica para trabajar de manera articulada la prevención de delitos (Boroadhurst, et. al., 2015). Esta investigación especializada está liderada por los administradores de justicia y los operadores de seguridad ciudadana para prevenir de manera integral la ciberdelincuencia (Howel, et. al., 2017). Quiere decir, que la investigación integral y especializada está representada por la fiscalía de delitos cibernéticos, como encargados de investigar, analizar y sancionar este tipo de delitos, realizando un trabajo conjunto con otras instituciones, empresas y los mismos ciudadanos.

Así mismo, se tiene la prevención e investigación de la ciberdelincuencia, está referido a las acciones de las personas, empresas y el Estado para generar planes de seguridad de protección de datos e información personalizada, con barreras para el acceso a la información, para limitar el alcance a la delincuencia (Boroadhurst, et.al., 2015). Y respecto a la investigación de la fiscalía especializada y otros operadores de justica realizan, deben contar con herramientas tecnológicas eficientes para rastrear este tipo de delincuencia, con equipos y tecnología eficiente para investigación y sanción respectivo.

En ese sentido, el tema de prevención debe ser integral, dado que los delitos operan desde el anonimato, fuera del lugar donde cometen el crimen, no tienen un acercamiento directo con la víctima (Ortíz y López, 2024). Por esa razón, la ciberdelincuencia es abordado por las autoridades desde el ámbito legal, buscando la culpabilidad de estos delitos con investigación profunda, con políticas públicas eficientes y presupuesto para mitigar este tipo de delitos (Howel, et. Al., 2017). Quiere decir, que la investigación que se da a los delitos cibernéticos, se realiza con el seguimiento del Estado y los operadores de justicia desde el punto de vista legal, buscando la paz social y seguridad ciudadana, dado que estos conllevan a pérdidas económicas y afectación psicológica de las víctimas. También, estos delitos escapan de las investigaciones policiales porque hay carencias de tecnología y presupuesto, conllevando que estos delitos superen fronteras interdisciplinarias, con investigaciones integrales en la parte jurídica, de formación, políticas económicas, de comunicación y sociológicas (Ortíz y López, 2024).

Las condiciones de prevención de ciberdelincuencia como las acciones ilegales, delictivas que van en contra de la Constitución y contra de los derechos de las personas, como es menoscabar o violar la privacidad del patrimonio o la información de las personas (Stratton, et al., 2017). En esta medida la prevención se da mediante acciones del ente rector para prevenir la delincuencia cibernética, usando mecanismos de protección de datos e información con las instituciones y empresas correspondientes.

También, se tiene la sanción de la ciberdelincuencia, se trata del proceso de las acciones que realizan los tomadores de decisiones de justicia para la indagación de los delitos, juntando las respectivas evidencias de los delitos cibernéticos, buscando una sanción respectiva de acuerdo a lo que indica la ley (Parkhomenko y Evdokimov, 2015). En esa medida, se debe tener en cuenta herramientas tecnológicas para poder investigar delitos cibernéticos, con previsiones legales respectivas a fin de garantizar los procesos correctos y efectivos (Sukharenko, 2019).

Así mismo, se tiene los siguientes aspectos conceptuales sobre la ciberdelincuencia como actos o acciones que contravienen la ley usando Tecnologías de Información y Comunicación (TIC) par cometer delitos en diferentes plataformas digitales, sin estar presentes físicamente en el lugar donde se comete el delito. De igual manera, también existe la ciberdelincuencia organizada que, según la Unodoc, está asociada a acciones ilícitas con ayuda de herramientas electrónicas, cibernética y tecnología en general para cometer dichas acciones que vulneran la tranquilidad de personas, organizaciones y el propio estado (Defensoría del Pueblo, 2023). En sí, estos delitos son tradicionales y de fácil acceso para los delincuentes, usando computadoras, redes sociales, o diferente tecnología informática o de comunicación. Además, este tipo de delitos se dan sin cometer esfuerzos más que el manejo del internet y de plataformas digitales para cometer acciones ilegales con el fin de beneficios personales de este tipo de delincuencia.

Además, jurídicamente, los ciberdelitos se enmarcan en el uso de las TIC, donde normativamente, la información es un bien jurídico que debe ser protegido por el estado y las instancias correspondiente, que es indispensable para que las personas se desarrollen, conformado por los pilares de confidencialidad, la integridad y la disponibilidad, por la que no debe ser violado por ninguna persona en ninguna de sus formas (Defensoría del Pueblo, 2023). Por otra parte, respecto a la obtención de información como elemento de prueba para la fiscalía especializada e investigar los ciberdelitos, debe ser la recolección de datos de manera preservada, analizada y presentada para el análisis digital correspondiente. Esta debe ser una acción impecable, con las herramientas correspondientes, de manera integral y coordinada, con principios de objetividad, legalidad, idoneidad e inalterabilidad. Además, se la evidencia digital para sancionar a los ciberdelitos debe estar almacenado es dispositivos con valor probatorio para poder realizar una investigación, analizarla y sancionarla; estas están sujetas a pruebas informáticas y electrónicas (Nessi, 2017).

En esa medida, la prevención de los ciberdelitos es importantes, teniendo en cuenta el uso de los dispositivos digitales como la geolocalización, para evitar que la delincuencia acceda a datos de ubicación, o evitar brindar micha información de datos personales en las redes sociales, para evitar ser

víctima de robo de información de chantaje o cualquier otro tipo de abuso (Ministerio de Justicia y Derechos Humanos, 2022).

También, en los delitos cibernéticos están conformados por diferentes tipos como: Hacker negro, es el tipo de delincuencia que usa las redes sociales, robando contraseñas, números de tarjetas de crédito, e información importante, usando el sistema o suplantando o borrando información para apoderarse de dinero ajeno. Hacker blanco, son conocidos como éticos, se meten en redes informáticas para detectar puntos débiles, para ellos se especializan en ciertos temas informáticos de organizaciones para ver qué tan vulnerable es su sistema y realizar recomendaciones. Hacker gris, es una combinación de hacker blanco y negro, que busca solucionar problemas de sistemas apropiados e de alguna información para pedir un cobro económico respectivo. Hacker rojo, usan sus competencias para apoyar a las organizaciones a luchar contra la ciberdelincuencia, conocidos como vigilantes de la seguridad (Flores, 2013).

2. Material y método

La investigación fue de tipo aplicada, teniendo en cuenta teorías existentes para fundamentar la investigación, de esa manera ampliar el conocimiento sobre la investigación integral y especializada para la prevención y sanción de la ciberdelincuencia.

Tuvo un enfoque cualitativo, sin recurrir a la cuantificación numérica para medir la variable, usando revisión sistemática de investigaciones a fines para estudiar el problema y describirlo a nivel internacional y nacional en función a los objetivos. El diseño fue descriptivo simple, con revisión de literatura mediante artículos científicos, con amplia exploración de manera cohesiva, mediante revisión holística sobre la investigación integral y especializada para la prevención de la ciberdelincuencia.

Respecto a las fuentes de selección de datos, se uso base de datos de alto impacto como Scopus, Web Of Science Scielo de los últimos cinco años, priorizando fuentes de artículos con acceso al documento completo en referencia a los objetivos desde el general y los específicos. Este criterio de rigurosidad fue muy relevante y las fuentes confiables. La muestra estuvo considerada por artículos científicos de revistas indexadas de los últimos cinco años. La técnica fue la revisión sistemática y el instrumento fue la guía de análisis.

Respecto al volumen de publicaciones, en un inicio se buscó 120 artículos en relación al tema de investigación; luego se tuvo en cuenta los criterios de exclusión en función al tema de investigación se quedó con 80 artículos, luego se tuvo en cuenta los últimos 8 años, quedándose con 40 artículos. Luego se tuvo en cuenta la selección de artículos en función a los objetivos, quedándose con 30 artículos; Luego se selección artículos de los últimos 5 años, quedándose con 18 artículos en total.

Así mismo, respecto a los aspectos éticos se tuvo en cuenta la justicia, teniendo en cuenta y considerando a los autores que participaron en la investigación (Autor y asesor). Así mismo, se tuvieron en cuenta el turnitin para evitar anti plagio. Así mismo, se tuvo en cuenta las citas en función al APA séptima edición.

3. Resultados

Los resultados fueron colocados en tablas de análisis con los datos de los autores, título, ubicación, y el desarrollo de cada investigación en el siguiente detalle:

O.E.1. Describir la investigación integral y especializada de la ciberdelincuencia.

Tabla 1

Investigación integral y especializada de la ciberdelincuencia

Autor	Metodología	Resultados y conclusiones
Díaz, et. al. (2023)	El trabajo fue aplicado, de nivel descriptivo analítico y enfoque cualitativo	Obtuvo que él ciberdelincuente tiene algunas características narcisistas, que busca apoderarse de información de datos para chantajear a sus víctimas con su modo operandi de despreocupación y modernización de formas y medios para delinquir en 37%. En Colombia los expertos de la Dirección de Investigación Criminal e INTERPOL, obteniendo que las tecnologías de información y comunicaciones forman parte del ciberespacio pero que tienen efecto en la parte física de las personas considerado en un análisis matricial. Además, se tuvo en cuenta en contraste con las teorías del control social se han abordado actos ciber delincuenciales de manera formal, donde el Estado cumple con la normativa, sin embrago carece de herramientas y presupuesto para hacer cumplir las leyes implementado acciones para investigar y prevenir ciberdelitos que atormentan a la población.
López (2022)	El trabajo fue descriptivo hermenéutico, usando análisis documental como técnica y la guía de análisis como instrumentos, de enfoque cualitativo.	Encontrando que los delitos cibernéticos se atribuyen a las teorías absolutas o retributivas, en la que los delitos de esta índole su culpabilidad en superior y a arrea grandes consecuencias, sin embrago las sanciones son débiles en el marco penal, viéndose reducido el delito a una contribución para las víctimas con justificaciones que avalan prácticamente al que comete el delito. Además, referente a la finalidad preventiva general del delito de la ciberdelincuencia fue menor al espacio físico tradicional en 32%, en la que a pesar de existir un alista larga de crímenes similares no hay espacios de alta tecnología de persecución e identificación de identidad de este tipo de delincuentes en 041%, rebajando la eficacia de los procesos y castigos, que siguen intimidando a sus víctimas. En conclusión, no se han desarrollado procesos específicos y eficientes para prevenir la ciberdelincuencia.
Ávila (2024)	Trabajo descriptivo, de enfoque mixto, usando el análisis normativo como técnicas.	Encontró que, la tipificación del delito ciber delincuencial está en el marco del convenio Budapest dentro de la normativa internacional, por ello, la ciberdelincuencia no tiene una normativa específica si no general y amplia. Concluyendo que a pesar que la ciberdelincuencia trae consigo consecuencias diversas que muchas veces el propio sujeto que con engaños hace que el delincuente acceda a datos confiables, que luego sacan provecho de la misma, sin muchas veces ser detectados o castigados legalmente.
Estrada (2024)	Trabajo con enfoque mixto, básica, con análisis de normativa de	En la legislación peruana se observa mucha impunidad de delitos informáticos, identificando factores para no llegar a una sanción a este tipo de delincuencia, dentro

	cibercrimen.	de ellos figura la no individualización de este tipo de delito, conllevando al archivo de los procesos. Al darse este tipo de casos, el sujeto en cuestión no es considerado como hecho constituido de manera individual y el proceso legal de investigación exige una plena individualización, por ende, no se puede seguir con el hecho de manera formal; además existen vacíos legales que dejan impunes los casos. Concluyendo que, la delincuencia está ganado al ordenamiento jurídico, con defiende tecnología de delitos para investigación de manera integral y sancionar estos delitos que dañan a la sociedad.

Fuente. Revisión de artículos de literatura

La tabla muestra la investigación integral y especializada de la ciberdelincuencia, en la que el 70% de autores indica que existe una débil investigación integral y especializada para investigar a la ciberdelincuencia, en la que los delincuentes aprovechan el descuido de exhibición de información personal para su apoderamiento para delinquir de diferentes maneras; sin embargo, la investigación a este tipo de delitos está asociada a las tecnologías de información como medio para delinquir dentro del ciber espacio. Las mismas están asociadas a las teorías de control social, absolutas o retributivas, donde el estado es el ente rector de la normativa, pero carece de herramientas y recursos para su implementación especializada, donde las sanciones son débiles por no ser considerado un daño de espacio físico, avalando al que comete el delito. El 30% indica que el marco normativo de los delitos cibernéticos está tipificado en modelos internacionales dentro del convenio de Budapest, que no se asemejan a nuestra realidad, sin embargo, ello no es una normativa específica si no muy general, quedando impunes los delitos informáticos, por ser considerados delitos no individualizados que no se formalizan en los procesos legales. Ello hace que no haya una investigación integral donde participe el estado, los ciudadanos e instituciones para cooperar en herramientas especializadas e investigar la ciberdelincuencia.

O.E.2. Describir el proceso de prevención y sanción de la ciberdelincuencia.

Tabla 2

Proceso de prevención sanción de ciberdelincuencia

Autor	Metodología	Resultados y conclusiones
Castillo (2023)	Investigación aplicada, enfoque cualitativo y diseño no experimental.	Identificó que existe una alta adaptación tecnológica, con ciberactividad, con uso contante de internet y redes; ello a conllevado que el vandalismo en robo de datos se ha incrementado. Además, hay mucha exposición de información de datos, que son extraídos por personas inescrupulosas para aprovecharse y tener al asecho a sus víctimas, donde los delincuentes usan métodos sofisticados para apoderase de la información, métodos y tecnología que carece la policía para prevenir y sancionar estos casos. La ciberdelincuencia no solo afecta el ciberespacio, si no tiene graves consecuencias en el espacio físico, para ello la prevención y ciberseguridad de información es necesaria.
Mayer y Óliver (2020)	La investigación fue descriptiva analítica, de enfoque cualitativa,	Los resultados analizados mostraron que, a pesar de la cantidad de teorías en materia de fraude informático o ciberdelitos, aún no se han aplicado teorías específicas

	usando el análisis hermenéutico.	en materia legal para prevenir este tipo de casos. En la mayoría de casos estos delitos quedan impunes, dado que hay etapas como de ejecución imperfecta o actos preparatorios de fraude por formar parte de categoría de hackeo o sabotaje informático, por la que la normativa debe ser tajante y específica para castigar este tipo de conductas como delitos informáticos, en ese sentido las teorías y las normativas deben ampliarse regulando tres requisitos copulativos verificando la conducta manipulativa, la provocación del delito y el fin de lucro de la acción en perjuicio del patrimonio institucional o personal.
Pérez y Rodríguez (2023)	El trabajo fue de enfoque mixto, descriptivo sistemático, con análisis documental	En sus resultados encontró que existe pocos estudios de investigaciones sociales interdisciplinarios. Además, se encontró que se han tomado falsas creencias sobre la seguridad en línea, desvirtuando la interpretación de manera individual o en conjunto, aduciendo que las víctimas de robos cibernéticos son responsables de brindar información específica o delicada para el delincuente, y el segundo son personas anónimas que no se pueden investigar ni sancionar, para ello se debe realizar investigaciones explicativas que demuestren la normativa con el mundo real, con tecnología que identifique al victimario. Concluyendo que existen muchos hechos de delitos cibernéticos que se trasladan del espacio físico al ciberespacio, sin embargo, no son sancionados por la falta de recursos de los administradores de justicia y la cantidad de delitos cometidos y el escaso apoyo social.
Gomero y Sánchez (2024)	Trabajo descriptivo simple, de enfoque mixto, usando la cantidad de denuncias y expedientes de delitos cibernéticos.	Los resultados mostraron los establecimientos de salud, el 80% tuvo planes respondiendo inmediatamente a este tipo de delitos, garantizando buenas acciones de ataques cibernéticos, buscando proteger la información y los datos, colocándolos con copias los datos vulnerables y críticos en diferentes establecimientos de salud; además siempre realizaban visitas inopinadas y otros operativos con softwares de seguridad para resguardar los datos, de esa manera prevenir robos o ciberataques delincuenciales. Concluyendo que existe gestión informática reactiva ante los ataques delincuenciales, dado que el país carece de reglas y herramientas normativas y presupuestales para castigar este tipo de delitos sin que haya perjuicios críticos en el espacio físico, por ello la importancia de la ciberseguridad debido a la transformación digital en que vivimos.

Fuente. Revisión de artículos de literatura

La tabla muestra el proceso de prevención y sanción de los delitos cibernéticos, en la que el 50% de autores coinciden que los ciberdelitos se dan por la ciberactividad, la conectividad, el internet, que facilita la exposición de datos, donde cada vez la delincuencia va ganando terreno para aprovecharse de los ciudadanos e instituciones, valiéndose de herramientas tecnológicas cada vez mas sofisticadas para delinquir, haciendo daño a los ciudadanos, ya que no solo se traba del ciberespacio, si no que trasciende el espacio físico las víctimas; sin embargo la mayoría quedan impunes al no contar con

herramientas tecnológicas sofisticadas, para ello se debe prevenir con la ampliación de tres requisitos en la normativa como la copulativa, la conducta manipuladora y la provocación del delito con fines de lucro de los ciudadanos e instituciones. El 50% de autores concuerdan que el fraude informático no cuenta con material legal específico dentro de la normativa de países menos implementados tecnológicamente para prevenir y sancionar delitos cibernéticos, considerándose una ejecución imperfectos dentro de los delitos preparatorios, incluso protege al delincuente aduciendo que se basó en la exposición de datos de las víctimas, provocando los hechos, para ello en modo de prevención, los ciudadanos e instituciones deben proteger los datos de manera continua, para evitar ser sorprendidos, dado que la normativa tiene vacíos legales, que hacen que no se castiguen estos hechos, tampoco hay apoyo social para castigar estos delitos.

O.G. Conocer cómo se realiza la investigación integral y especializada en la prevención y sanción de la ciberdelincuencia en la prevención y sanción de la ciberdelincuencia.

Tabla 3

Investigación integral y especializada en la prevención y sanción de la ciberdelincuencia

Autor	Metodología	Resultados y conclusiones
Ospina y Sanabría (2020)	Descriptivo hermenéutico, enfoque cualitativo y nivel descriptivo analítico.	Dentro de los resultados obtuvo que existen muchas denuncias cibernéticas en apoderamiento de datos en 34% y robos de las cuentas de los usuarios de bancos en 38%, donde la población presenta mucha vulnerabilidad ante este tipo de delitos, A pesar de existir legislación general, no hay legislación sólida en materia de seguridad o protección de información, hay carencia de barreras para acceso a información por parte de terceros o codificación de información extrema. En conclusión, no se ha implementado softwares especializados a la política para poder detectar y prevenir delitos cibernéticos, con tecnología deficiente para sancionar estos delitos que cada día van incrementándose en la ciudad. Tampoco hay mapas de riesgos donde se dan más estas amenazas usando información del ciudadano.
Padalka (2022)	El trabajo fue aplicado, de nivel analítico hermenéutico, analizando normativa ucraniana.	En Ucrania abunda el ciber espionaje con ciberataques al Estado, a las empresas y ciudadanos, apropiándose de datos, y dinero de cuentas bancarias, esto se da por agencias de otros países, siendo delitos con fines de lucro para estas organizaciones que atemorizan a Ucrania, con sistemas modernos que son detectados para la prevención respectiva. Hay respuesta inmediata a estas ciber amenazas, con investigaciones policiales inteligentes forenses. Además, en la parte normativa es muy eficiente para sancionar internamente en el país este tipo de delitos, sin embrago es complicado sancionar bandas criminales externas, por ello el Estado se prepara para la preparación de protección de datos e información delicada y evitar este tipo de problemas.
Arapa, et. al. (2024)	El enfoque fue mixto, de nivel descriptivo hermenéutico, también se uso la base de datos	Los resultados mostraron que hubo un incremento considerable de la ciberdelincuencia; además se reportó información irregular de los delitos denunciados con desinformación, escasa herramientas

	de denuncias.	en tecnología de la policía y falta de conciencia para la prevención por parte del gobierno y las empresas, con una precaria ciberseguridad, las víctimas son generalmente ciudadanos de entre 27 a 59 años de edad en 55%. Concluyendo que la información excesiva de las personas en las redes, o la exposición de datos de cuentas bancarias, hace que haya una gran tendencia a convertirse en víctimas, y muchas veces los delitos quedan impunes por carecer de aplicación de normativa firme o no contar con tecnología de punta para identificar los responsables.
Ruíz y Solís (2024)	El trabajo tuvo enfoque mixto, de nivel descriptivo analítico, usando denuncias como muestra y normativa del Perú en caso de delitos cibernéticos.	Los resultados mostraron que los robos cibernéticos se dan mediante envío de correos a las víctimas para apoderase de información oportuna para extorsionarlos en 37%, o bajo la modalidad de enlaces masivos con virus en 49%, o suplantan páginas de entidades financieras en 29%, donde solicitan datos específicos y puntuales de los clientes y los códigos CCI, teléfonos y claves token para apoderarse de dinero de las cuentas bancarias. Además, siempre estos delitos quedan impunes por la no detección ni prevención por parte de la policía, perdiendo sus ahorros de trabajo los ciudadanos, faltando a su derecho de vivir en un espacio de paz y desarrollo. Concluyendo que los ciudadanos deben cuidar su información y corroborar enlaces sospechosos que soliciten datos personales o confidenciales, evitar compartir información que pueda generar infiltraciones en sus datos que serán perjudiciales.
Ramírez, et. al. (2022)	El trabajo fue aplicado, de enfoque cuantitativo, usando encuestas como técnica y cuestionario a víctima de robo cibernético.	Resultando que hubo cuatro tipos de ciberdelitos como phishing, spamming y otra forma de sotfware antivirus de acoso en las redes; además, existen causas de relaciones de parejas entre facultades como causa del bullying en las redes, sin embrago la mayoría de facultados no tienen conciencia del ciberdelito, usando la discriminación, la mofa y cualquier otra excusa para apoderarse de datos cibernéticamente, con una influencia de 0.89, 0.75, y 074 entre todos los delitos. Concluyendo que existe relación directa entre el ciberdelito y la conciencia de los estudiantes, pero se necesitan mayares herramientas para castigar legalmente este tipo de delitos, aunque parezcan no muy fuertes como la ciberdelincuencia de organizaciones criminales.

Fuente. Elaboración a partir de antecedentes de revisión sistemática

La tabla muestra la investigación integral y especializada en la prevención y sanción de la ciberdelincuencia, el 70% de autores concuerda que dentro de las investigaciones se tuvo denuncias de robos de información masiva, entre las víctimas fueron ciudadanos con apoderamiento de información de cuentas, datos personales, en cambio las empresas perdieron información valiosa de clientes y las entidades financieras información de clientes; si embargo la mayoría de países carece de carece de normativa específica y sólida para sancionar los delitos, sumado al hecho de carecer de herramientas especializadas para investigar este tipo de delitos que vulnera los derechos de los ciudadanos. El 30% de autores indica que en algunos países desarrollados se dan los delitos cibernéticos mas en grandes

empresas, y a los ciudadanos solo de manera regular, dado que existen hackers más selectivos para robo de información de instituciones como salud, el sector financiero y otras empresas, que usan dicha información para armar estrategias de competencia en el mercado; a pesar que hay una relación directa, estos países usan el tema de codificación extrema de sus datos a modo de prevención, ya que a pesar que en países desarrollados hay normas sólidas para sancionar estos delitos, es complicado tratar con bandas criminales externas que no radican en el país: En sí, no siempre la investigación integral y especializada previene delitos de ciberdelincuencia, menos se sancionan a cabalidad.

4. Discusión

Referente al objetivo específico 1, el 70% de autores indica que existe una débil investigación integral y especializada para investigar a la ciberdelincuencia, en la que los delincuentes aprovechan el descuido de exhibición de información personal para su apoderamiento. El 30% indica que el marco normativo de los delitos cibernéticos está tipificado en modelos internacionales, que no se asemejan a nuestra realidad, sin embargo, ello no es una normativa específica si no muy general, quedando impunes los delitos informáticos. En discusión con Entralgo, et. al. (2014), indica que la teoría de la pena indica que el estado es el ente rector normativo de cada país y los administradores de justicia deben velar por la seguridad de los ciudadanos del país, con investigaciones reales e instrumentos pertinentes en articulación con todos los involucrados para investigar delitos de manera especializada. En ese sentido, en concordancia con Carrera, et. al. (2020), la investigación integral especializada de la ciberdelincuencia ayuda a identificar medio probatorios de los delitos, donde los operadores de justicia de manera integral ayudan en los procesos de organización, e identificación de los medios probatorios para demostrar el hecho del delito. Por otra parte, la investigación especializada considerada en el código procesal penal, en la que los operadores de justicia deben tener elementos normativos o herramientas con oportunidad de descargo del imputado para poder practicar la justicia (Meléndez, et. al., 2021). Las teorías indicadas no se asemejan a los resultados indicados por los autores dentro de la investigación, en la que no se cumplen las teorías y la normatividad de los países menos desarrollados, existiendo una débil investigación integral y especializada para atender a la ciberdelincuencia.

Respecto al objetivo específico 2, el 50% de autores coinciden que los ciberdelitos se dan por la ciberactividad, la conectividad, el internet, que facilita la exposición de datos, donde cada vez la delincuencia va ganando terreno para aprovecharse de los ciudadanos e instituciones. El 50% de autores concuerdan que el fraude informático no cuenta con material legal específico dentro de la normativa de países menos implementados tecnológicamente para prevenir y sancionar delitos cibernéticos. En discusión con Boroadhurst, et. al. (2015), la prevención e investigación de la ciberdelincuencia tiene que ver con el involucramiento del estado, las personas, empresas e instituciones en general, con la finalidad de proteger datos e información específica, con barreras altas de acceso para limitar el alcance delincuencial. También, la prevención integral debe ser sumamente alta y delicada, dado que los delincuentes operan desde el anonimato y lejos del lugar físico de donde ocurren los hechos, sin tener un acercamiento con la víctima (Ortiz y López, 2024). En discusión con la teoría de la garantía procesal, los derechos fundamentales de los ciudadanos amparados en la constitución, donde solicita al sistema de justicia las medidas de protección o búsquedas de justicia para una mayor tranquilidad de los ciudadanos, más que toda la influencia de los organismos a fines o rectores para prevenir y sancionar situaciones de delitos (Polyakov, 2019). Sin embargo, ello no refleja los resultados de los autores dentro del trabajo investigativo, dado que el estado no realiza un verdadero trabajo de prevención de la ciberdelincuencia, tampoco hay una sanción ejemplar, dado el sistema judicial no cuenta con herramientas tecnológicas especializadas para realizar una verdadera investigación, sumándose a los limitados recursos económicos para investigación y sanción respectiva.

En función al objetivo general el 70% de autores concuerda que dentro de las investigaciones se tuvo denuncias de robos de información masiva; sin embargo, la mayoría de países carece de normativa específica y sólida para sancionar los delitos. El 30% de autores indica que en algunos países desarrollados se dan los delitos cibernéticos más en grandes empresas, y a los ciudadanos solo de manera regular. En discusión con Howel, et. al. (2017), la investigación integral y especializada debe

estar liderada por los administradores de justicia para prevenir de manera integral la delincuencia. Ésta está representada por la fiscalía de delitos cibernéticos, como encargados de investigar, analizar y sancionar este tipo de delitos, realizando un trabajo conjunto con otras instituciones, empresas y los mismos ciudadanos. Respecto a la sanción de la ciberdelincuencia está basada en procesos de acciones o decisiones que realizan los operadores de justicia para indagar delitos, juntando evidencias para la sanción correspondiente (Parkhomenko y Evdokimov, 2015). En concordancia con Poaquiza, et. al. (2020), en el principio de objetividad, indica que los entes rectores de justicia buscan la verdad de los hechos en una investigación, buscando los medios probatorios contundentes amparados dentro de la constitución y las normas. También, está el principio de investigación previa, pues se debe ajustar a la objetividad y al cumplimiento de las normas legales, sin pasar por encima de los derechos de los ciudadanos, con los tiempos correspondientes para los descargos del imputado y determinar un veredicto justo (Ortíz y López, 2024). En sí, no siempre la investigación integral y especializada previene delitos de ciberdelincuencia, menos se sancionan a cabalidad, dado que hay carencia de

5. Conclusiones

La investigación integral y especializada en la prevención y sanción de la ciberdelincuencia, el 70% de autores concuerda que dentro de las investigaciones se tuvo denuncias de robos de información masiva; sin embargo, la mayoría de países carece de normativa específica y sólida para sancionar los delitos, sumado al hecho de carecer de herramientas especializadas para investigar este tipo de delitos que vulnera los derechos de los ciudadanos. El 30% de autores indica que en algunos países desarrollados se dan los delitos cibernéticos más en grandes empresas, y a los ciudadanos solo de manera regular, dado que existen hackers más selectivos para robo de información. A pesar que hay una relación directa, estos países usan el tema de codificación extrema de sus datos a modo de prevención, ya que a pesar que en países desarrollados hay normas sólidas para sancionar estos delitos, es complicado tratar con bandas criminales externas que no radican en el país: En sí, no siempre la investigación integral y especializada previene delitos de ciberdelincuencia, menos se sancionan a cabalidad.

La investigación integral y especializada de la ciberdelincuencia, el 70% de autores indica que existe una débil investigación integral y especializada para investigar a la ciberdelincuencia, en la que los delincuentes aprovechan el descuido de exhibición de información personal para su apoderamiento para delinquir de diferentes maneras; sin embargo, la investigación a este tipo de delitos está asociada a las tecnologías de información como medio para delinquir dentro del ciber espacio**.** El 30% indica que el marco normativo de los delitos cibernéticos está tipificado en modelos internacionales dentro del convenio de Budapest, que no se asemejan a nuestra realidad, sin embargo, ello no es una normativa específica si no muy general, quedando impunes los delitos informáticos, por ser considerados delitos no individualizados que no se formalizan en los procesos legales. Ello hace que no haya una investigación integral donde participe el estado, los ciudadanos e instituciones para cooperar en herramientas especializadas e investigar la ciberdelincuencia.

Respecto al proceso de prevención y sanción de los delitos cibernéticos, el 50% de autores coinciden que los ciberdelitos se dan por la ciberactividad, la conectividad, el internet, que facilita la exposición de datos, donde cada vez la delincuencia va ganando terreno para aprovecharse de los ciudadanos e instituciones, valiéndose de herramientas tecnológicas cada vez más sofisticadas para delinquir, haciendo daño a los ciudadanos, ya que no solo se traba del ciberespacio, si no que trasciende el espacio físico las víctimas. El 50% de autores concuerdan que el fraude informático no cuenta con material legal específico dentro de la normativa de países menos implementados tecnológicamente para prevenir y sancionar delitos cibernéticos, considerándose una ejecución imperfectos dentro de los delitos preparatorios, para ello en modo de prevención, los ciudadanos e instituciones deben proteger los datos de manera continua, para evitar ser sorprendidos, dado que la normativa tiene vacíos legales, que hacen que no se castiguen estos hechos, tampoco hay apoyo social para castigar estos delitos.

6. Referencias

Arapa-Ticona, J. C., Cari-Calcina, K. M., Laura-Lipe, J. J., Laura-Valero, M., Merma-Cabrera, R. M., Tarapa-García, H. L., & Condori-Parí, N. (2024). Causas y consecuencias del incremento de los delitos informáticos en la ciudad de puno 2023. *Revista de derecho*, 9(1), 6-22. https://doi.org/10.47712/rd.2024.v9i1.262

Astorayme, J.L. (2023). *Ciberdelincuencia y la implementación de Fiscalías Especializadas en San Juan de Miraflores, 2022*. [Tesis de posgrado, Universidad César Vallejo]. Repositorio UCV. Chrome extension://efaidnbmnnnibpcajpcglclefindmkaj/https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/121896/Astorayme_SJLSD.pdf;jsessionid=649472D5E94E1546A539AF6DC95C6736?sequence=1

Ávila-Trivelli, A.A. (2024). Análisis al delito de fraude informático analisystocomputer-Relatedfraud. *VOXJURIS, Lima*, 42(1),159-173. https://doi.org/10.24265/voxjuris.2024.v42n1.13

Broadhurst, R. Grabosky, P., Alazab, M. & Chon, S. (2014). Organizations and Cyber crime: An Analysis of the Nature of Groups engaged in Cyber Crime International Journal of Cyber Criminology, 8(1), 1-20. https://www.researchgate.net/publication/288262190_Organizations_and_cyber_crime_An_analysis_of_the_nature_of_groups_engaged_in_cyber_crime

Castillo-García, J. (2023). Análisis de la ciberseguridad en espacios educativos pertenecientes a la Fuerza Aeroespacial Colombiana. *Ciencia y Poder Aéreo*, 19(1), 137-151. https://doi.org/10.18667/cienciaypoderaereo.803

Carbajal, M. (2022). *Las fiscalías especializadas en delitos informáticos como mecanismo para la lucha contra el cibercrimen*. (Tesis de posgrado, Universidad San Martín de Porres). Repositorio USMP. Chrome extension://efaidnbmnnnibpcajpcglclefindmkaj/https://repositorio.usmp.edu.pe/bitstream/handle/20.500.12727/11398/carbajal_cm.pdf?sequence=1&isAllowed=y

Carrera-Calderón, F. A., Cadena-Sayavedra, H. F.; Cepeda-Luna, C. D.; Alvarado-Villavicencio, M. S. Crimes on the deep web and their effects on cyber victims against Ecuadorian legislation. Revista digital de Ciencia, Tecnología e Innovación, 7(12), pp. 1263-1275. https://revista.uniandes.edu.ec/ojs/index.php/EPISTEME/article/view/2301

Defensoría del Pueblo (2023). *La ciberdelincuencia en el Perú: estrategias y retos del Estado*. [Informe en línea]. Lima, Perú. Chrome

extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.defensoria.gob.pe/wp-content/uploads/2023/05/INFORME-DEF-001-2023-DP-ADHPD-Ciberdelincuencia.pdf

Díaz-Samper, G. A. J., Molina-Garzón, A. L., & Serrador-Osorio, L. E. (2023). Aproximación al ciberdelincuente desde la perspectiva del control social. *Revista Criminalidad*, 65(3), 81-95. https://doi.org/10.47741/17943108.508

Entralgo, J., Salager-Meyer, F., & Luzardo-Briceño, M. (2014). Títulos de artículos de investigación científica escritos en inglés: un estudio interdisciplinario. *Núcleo*, 26(31), 75-100. http://ve.scielo.org/scielo.php?script=sci_arttext&pid=S079897842014000100003&lng=es&tlng=es.

Flores-Quispe, C. A. (2013). Tipos de hackers. *La Paz*, 8(3), 16-22. http://revistasbolivianas.umsa.bo/pdf/rits/n8/n8a08.pdf

Gomero-Cuadra, R., & Sánchez-Calle, D. (2024). Ciberseguridad en servicios de apoyo al médico ocupacional de la ciudad de Lima. Estudio piloto. *Revista Médica Herediana*, 35(1), 38-43. https://dx.doi.org/10.20453/rmh.v35i1.5298

Howell, C.J., Maimon, D., Cochran, J.K., Jones, H.M., Powers, R.A. (2017). System Trespasser Behavior after Exposure to Warning Messages at a Chinese Computer Network: An Examination. International Journal of Cyber Criminology, 11(1), 63–77. https://www.cybercrimejournal.com/pdf/Howelletalvol11issue1IJCC2017.pdf

Jiménez-Prado, S. E., & Medina-Chicaiza, R. P. (2023). Internet de las cosas para la experiencia de compra en tiendas físicas. *Universidad, Ciencia y Tecnología*, 27(120), 31-41. https://doi.org/10.47460/uct.v27i120.729

Kolesnikov, N. (20 de mayo del 2024). *50 estadísticas clave de ciberseguridad para junio de 2024*. [Blog en línea], Madrid. https://www.techopedia.com/es/estadisticas-ciberseguridad.

Leyva-Serrano, C. (2021). Estudio de los delitos informáticos y la problemática de su tipificación en el marco de los convenios internacionales. (2021). *Lucerna Iuris Et Investigativo*, 1, 29-47. https://doi.org/10.15381/lucerna.v0i1.18373

López-Gorostidi, J. (2022). Sobre el alcance de los fines de la pena en el fenómeno criminal de la ciberdelincuencia. *Revista chilena de derecho y tecnología*, 11(1), 121 146. https://dx.doi.org/10.5354/0719-2584.2022.60913

Mayer-Lux, L., & Oliver-Calderón, G. (2020). El delito de fraude informático: concepto y delimitación. *Revista chilena de derecho y tecnología*, 9(1), 151 184. https://dx.doi.org/10.5354/0719-2584.2020.53447

Meléndez-Carballido, R., Carrión-León, K. E., Alfaro-Matos, M., & Paronyan, H. (2021). Effective Judicial Protection and the Principle of Objectivity of the fiscal investigation as a guarantee of its compliance. *Dilemas contemporáneos: educación, política y valores*, 9(1), 00072. https://doi.org/10.46377/dilemas.v9i.2980

Ministerio de Justicia y Derechos Humanos (2022). *Ciberdelincuencia reporte de información estadística y recomendaciones para la prevención*. [En línea]. Lima, Perú. efaidnbmnnnibpcajpcglclefindmkaj/https://cdn.www.gob.pe/uploads/document/file/3562747/Reporte%20de%20Ciberdelincuencia.pdf.pdf

Natalucci, F., Mahvash S. Qureshi, F. (10 de abril del 2024). *Las crecientes amenazas cibernéticas, una grave preocupación para la estabilidad financiera*. [Blog en línea] Fondo Monetario Internacional. https://www.imf.org/es/Blogs/Articles/2024/04/09/rising-cyber-threats-pose-serious-concerns-for-financial-stability

Nessi, A.M. (2017). *Manual de evidencia digital*. [Manual de evidencia digital]. Lima, Perú. efaidnbmnnnibpcajpcglclefindmkaj/https://www.mpfn.gob.pe/Docs/0/files/manual_evidencia_digital.pdf

Ortiz-Cervantes, M. V., & López-Soria, Y. (2024). The theory of crime and the concept of crime: a comparative perspective between the United States and Ecuador. *MQRInvestigar*, 8(2), 1406–1421. https://www.investigarmqr.com/ojs/index.php/mqr/article/view/1300/4591

Ospina-Díaz, M. R., & Sanabria-Rangel, P. E. (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=S1794310820200002001 99&lng=en&tlng=es.

Parkhomenko, S.V. Evdokimov, K.N. (2015). Computer Crime Prevention in the Russian Federation: Integrative and Integrated Approaches. *University of Economics and Law*, 2(6), 265-276. https://www.researchgate.net/publication/283125684_Prevention_of_cybercrime_in_the_Russian_federation_An_integrative_and_comprehensive_approaches

Padalka, A. (2022). Forensic and technical criminalistics support in cybercrime investigation: Countering cyber threats in Ukraine. *Revista Científica General José María Córdova*, 20(38), 407-423. https://doi.org/10.21830/19006586.901

Pérez-Martínez, A., & Rodríguez-Fernández, A. (2024). Implicaciones para las ciencias sociales del análisis de estafas y pederastia en línea en Ecuador. *Revista Rupturas*, 14(1), 145-164. https://dx.doi.org/10.22458/rr.v14i1.5183

Poaquiza, A., Galarza, C. y Quiroga, M. (2020). La investigación integral y su incidencia en el principio de objetividad en la acción penal. *Universidad, Ciencia y Tecnología*, 24(100), 37-43. http: ://301-article-896-1-10-20200517%20(2).pdf

Polyakov, V. (2019). Criminalistics specifics of methods of committing computer crimes and peculiarities of their prevention. *Revista de Ciencias Sociales y Humanidades*, 4(21), 90-97. https://dialnet.unirioja.es/servlet/autor?codigo=5556042

Ramírez-Asís, E. H., Figueroa-Norabuen, R. P., Quiñones-Toledo, R. E., & Márquez-Mázmela, P. Henostroza, R. (2022). Validación de una escala de conciencia sobre ciberdelito en estudiantes universitarios de Perú. *Revista Científica General José María Córdova*, 20(37), 208-224. 0https://doi.org/10.21830/19006586.791

Ruiz, P., y Solís-Castillo, C. (2024). Fraude informático en la modalidad de ciberdelincuencia en Lima. *Escpogra PNP*, 3(2), 143-155. https://doi.org/10.59956/escpograpnpv3n2.12

Stratton, G., Powell, A. and Cameron, R (2017). Crime and Justice in Digital Society: Towards a 'Digital Criminology'? International Journal for Crime, *Justice and Social Democracy*, 6(2), 17-33. https://www.researchgate.net/publication/317274183_Crime_and_Justice_in_Digital_Society_Towards_a_'Digital_Criminology'

Sukharenko, A.N. (2019). Russian ITC Security Policy and Cybercrime. *Ponars Eurasia,* 60(1), 1-7. chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.ponarseurasia.org/wp-content/uploads/attachments/Pepm601_Sukharenko_July2019_4.pdf

Vinelli Vereau, R. (2021). Los delitos informáticos y su relación con la criminalidad económica. *Lus Et Praxis*, 53(053), 95-110. https://doi.org/10.26439/iusetpraxis2021.n053.4995