



UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE DERECHO Y HUMANIDADES

ESCUELA PROFESIONAL DE DERECHO

**“Incremento de los delitos informáticos a consecuencia de la
pandemia del Covid-19 en la ciudad de Trujillo entre los años
2020-2021”**

TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE:

Abogado

AUTOR:

Flores Mori, Cesar Eugenio (orcid.org/0000-0003-3090-0301)

ASESORES:

Dra. Zevallos Loyaga, Maria Eugenia (orcid.org/0000-0002-2083-3718)

Dr. Rodriguez Casas, Luis Renato (orcid.org/0000-0001-9725-3001)

LÍNEA DE INVESTIGACIÓN:

Derecho Penal, Procesal Penal, Sistemas de Penas, Causas y Formas
del Fenómeno Criminal

LÍNEA DE RESPONSABILIDAD SOCIAL UNIVERSITARIA:

Fortalecimiento de la democracia, liderazgo y ciudadanía

TRUJILLO – PERÚ

2023

Dedicatoria

A Dios, por haberme permitido haber llegado a este momento tan importante en mi vida, por los triunfos y los momentos difíciles que me han enseñado a valorar cada día más.

A mis padres Cesar Eugenio Flores Montenegro y Juana Maribel Mori Espino que son el pilar de cada paso que doy y de cada esfuerzo y me brindan su apoyo incondicional para seguir con mis estudios académicos.

A mis hijos Ariana y Sebastián

Porque a su corta edad comprenden que a veces tenemos que sacrificar un poco de nuestro tiempo para lograr nuestros objetivos y metas.

Gracias al apoyo incondicional de mis tíos queridos Miguel Alvarado Vilela y Analí Magali Mori Espino por haber depositado toda su confianza en toda mi carrera universitaria.

y en especial a mi abuelo querido Eugenio Flores Mera por todas sus enseñanzas y consejos durante toda mi carrera universitaria y apostar por mis estudios.

AGRADECIMIENTO

*Agradezco a los doctores
Dra. María Eugenia Zevallos Loyaga
y al Dr. Luis Renato Rodríguez Casas
por la enseñanza y paciencia brindada,
pero sobre todo por el entusiasmo que
nos transmite para poder seguir adelante.*

*Gracias a los docentes que fueron un
ejemplo a seguir y han brindado su apoyo
para de esa manera
culminar mi tesis con satisfacción.*



UNIVERSIDAD CÉSAR VALLEJO

**FACULTAD DE DERECHO Y HUMANIDADES
ESCUELA PROFESIONAL DE DERECHO**

Declaratoria de Autenticidad del Asesor

Yo, ZEVALLOS LOYAGA MARIA EUGENIA, docente de la FACULTAD DE DERECHO Y HUMANIDADES de la escuela profesional de DERECHO de la UNIVERSIDAD CÉSAR VALLEJO SAC - TRUJILLO, asesor de Tesis titulada: "INCREMENTO DE LOS DELITOS INFORMATICOS A CONSECUENCIA DE LA PANDEMIA DEL COVID-19 EN LA CIUDAD DE TRUJILLO ENTRE LOS AÑOS 2020-2021.", cuyo autor es FLORES MORI CESAR EUGENIO, constato que la investigación tiene un índice de similitud de 9.00%, verificable en el reporte de originalidad del programa Turnitin, el cual ha sido realizado sin filtros, ni exclusiones.

He revisado dicho reporte y concluyo que cada una de las coincidencias detectadas no constituyen plagio. A mi leal saber y entender la Tesis cumple con todas las normas para el uso de citas y referencias establecidas por la Universidad César Vallejo.

En tal sentido, asumo la responsabilidad que corresponda ante cualquier falsedad, ocultamiento u omisión tanto de los documentos como de información aportada, por lo cual me someto a lo dispuesto en las normas académicas vigentes de la Universidad César Vallejo.

TRUJILLO, 21 de Junio del 2023

Apellidos y Nombres del Asesor:	Firma
ZEVALLOS LOYAGA MARIA EUGENIA DNI: 18190178 ORCID: 0000-0002-2083-3718	Firmado electrónicamente por: MZEVALLOS el 21- 06-2023 17:55:57

Código documento Trilce: TRI - 0546969





UNIVERSIDAD CÉSAR VALLEJO

**FACULTAD DE DERECHO Y HUMANIDADES
ESCUELA PROFESIONAL DE DERECHO**

Declaratoria de Originalidad del Autor

Yo, FLORES MORI CESAR EUGENIO estudiante de la FACULTAD DE DERECHO Y HUMANIDADES de la escuela profesional de DERECHO de la UNIVERSIDAD CÉSAR VALLEJO SAC - TRUJILLO, declaro bajo juramento que todos los datos e información que acompañan la Tesis titulada: "INCREMENTO DE LOS DELITOS INFORMATICOS A CONSECUENCIA DE LA PANDEMIA DEL COVID-19 EN LA CIUDAD DE TRUJILLO ENTRE LOS AÑOS 2020-2021.", es de mi autoría, por lo tanto, declaro que la Tesis:

1. No ha sido plagiada ni total, ni parcialmente.
2. He mencionado todas las fuentes empleadas, identificando correctamente toda cita textual o de paráfrasis proveniente de otras fuentes.
3. No ha sido publicada, ni presentada anteriormente para la obtención de otro grado académico o título profesional.
4. Los datos presentados en los resultados no han sido falseados, ni duplicados, ni copiados.

En tal sentido asumo la responsabilidad que corresponda ante cualquier falsedad, ocultamiento u omisión tanto de los documentos como de la información aportada, por lo cual me someto a lo dispuesto en las normas académicas vigentes de la Universidad César Vallejo.

Nombres y Apellidos	Firma
FLORES MORI CESAR EUGENIO DNI: 47910045 ORCID: 0000-0003-3090-0301	Firmado electrónicamente por: CFLORESMO92 el 28- 06-2023 22:41:12

Código documento Trilce: INV - 1304633



ÍNDICE DE CONTENIDOS

DEDICATORIA.....	ii
AGRADECIMIENTO.....	iii
DECLARATORIA DE AUTENTICIDAD DE ASESOR.....	iv
DECLARATORIA DE ORIGINALIDAD DEL AUTOR.....	v
ÍNDICE DE CONTENIDOS.....	vi
ÍNDICE DE TABLAS.....	vii
ÍNDICE DE ABREVIATURAS.....	viii
RESUMEN.....	ix
ABSTRACT.....	x
I. INTRODUCCIÓN.....	1
II. MARCO TEÓRICO.....	4
III. METODOLOGÍA.....	13
3.1. Tipo y diseño de investigación.....	13
3.1.1. Tipo de investigación.....	14
3.1.2. Diseño de investigación.....	14
3.2. Categorías, subcategoría y matriz de categorización.....	14
3.3. Escenario de estudio.....	15
3.4. Participantes.....	15
3.5. Técnicas e instrumentos de recolección de datos.....	15
3.6. Procedimiento.....	16
3.7. Rigor científico.....	16
3.8. Método de análisis de datos.....	16
3.9. Aspectos éticos.....	17
IV. RESULTADOS Y DISCUSIÓN.....	19
4.1 RESULTADOS.....	19
4.2 DISCUSIÓN.....	42
V. CONCLUSIONES.....	46
VI. RECOMENDACIONES.....	49
REFERENCIAS.....	50
ANEXOS.....	57

ÍNDICE DE TABLAS

TABLA 1: Incidencia de los delitos en materia de ciberdelincuencia Trujillo 2020-2021	18
TABLA 2: Acciones para combatir la ciberdelincuencia en la ciudad de Trujillo 2020-2021.....	21
TABLA 3: Roles de la entidad bancarías para buscar combatir la ciberdelincuencia.....	24
TABLA 4: Identificación de autores de los delitos cibernéticos en Trujillo 2020-2021.....	25
TABLA 5: Delitos informáticos en etapa de juzgamiento en la actualidad en Trujillo	26
TABLA 6: Procedimientos para la investigación de la ciberdelincuencia.....	26
TABLA 7: Nivel de aumento de los delitos cibernéticos entre los años 2020-2021	29
TABLA 8: Necesidad de una fiscalía especializada en ciberdelincuencia.....	31
TABLA 9: Capacitaciones y participación de los representantes públicos en los años 2020-2021 en Trujillo	33
TABLA 10: La logística que brinda las instituciones públicas para combatir los delitos informáticos en Trujillo	35

ÍNDICE DE ABREVIATURAS.

A:	Alcaldía
MP:	Ministerio Público
DIVINDAT:	División de delitos de alta tecnológica
PNP:	Policía nacional del Perú
DIVINCRI:	División de Crimines de la policía
ONU:	Organización de las naciones Unidas
CP:	Centro Poblado
ROF:	Reglamento De Organización y Funciones
UCV:	Universidad Cesar Vallejo
BCP:	Banco de crédito del Perú
DNI:	Documento Nacional de Identidad
INTERPOL:	Organización internacional de policía

RESUMEN

Esta investigación tuvo como objetivo general determinar las causales del incremento de delincuencia cibernética en tiempos de aislamiento social obligatorio producto del covid-19; teniendo un tipo de investigación básica, descriptiva, y un diseño basado en la teoría fundamentada. Así mismo se empleó el cuestionario de entrevista y la guía de análisis documental, que fueron validados por tres expertos y aplicados a 6 especialistas en derecho penal con competencia en delitos informáticos.

Los resultados obtenidos mostraron, que las principales causales de los delitos cibernéticos fueron la creación de la moneda digital como yape, plim y el desempleo por la pandemia del covid-19.

Se concluyó, que los delitos con mayor índice en el año 2020 al 2021 en la ciudad de Trujillo fueron el delito de suplantación de identidad y el fraude informático. El nivel aumento de ciberdelincuencia fue un 78% durante la pandemia. Como alternativas de solución se obtuvo que se necesitan herramientas digitales necesarias para desarrollar mecanismos para combatir la ciberdelincuencia, es por ello que el estado peruano debería realizar inversión para poder capacitar y tener herramientas digitales.

Palabras clave: Delincuencia cibernética, COVID-19, incremento.

ABSTRACT

The general objective of this investigation was to determine the causes of the increase in cybercrime in times of mandatory social isolation as a result of covid-19; having a type of basic, descriptive research, and a design based on grounded theory. Likewise, the interview questionnaire and the documentary analysis guide were used, which were validated by three experts and applied to 6 specialists in criminal law with competence in computer crimes.

The results obtained showed that the main causes of cybercrime were the creation of digital currency such as yape, plim and unemployment due to the covid-19 pandemic.

It was concluded that the crimes with the highest rate in the year 2020 to 2021 in the city of Trujillo were the crime of identity theft and computer fraud. The level of cybercrime increased by 78% during the pandemic. As solution alternatives, it was obtained that digital tools are needed to develop mechanisms to combat cybercrime, which is why the Peruvian state should invest in order to train and have digital tools.

Keywords: Cybercrime, COVID-19, increase.

I. INTRODUCCIÓN

En los últimos años, el derecho y la tecnología han provocado cambios dramáticos en el desarrollo de la sociedad, hoy en día el uso de la tecnología se ha vuelto crucial para la sociedad, lo que ha llevado al surgimiento de una nueva ciencia jurídica en el campo del derecho, como la ley de delitos informáticos. Las actividades delictivas con mayor índice en nuestro país son los fraudes informáticos, actividades que impliquen fraude, falsificación, daño, fraude sistemático, sabotaje, uso indebido de las computadoras, suplantación de identidad, extorciones y trata de blancas por tal motivo es necesario promover su regulación en el código penal. Debido a la dificultad para ubicar a los autores intelectuales de muchos delitos informáticos, lo que permite que muchos de ellos queden impunes y hace que la sociedad pierda paulatinamente la fe en la eficacia, eficiencia y oportunidad de la justicia en nuestro territorio peruano por carecer de las salvaguardas necesarias para proteger los intereses de nuestros ciudadanos, una de las razones del incremento de los delitos informáticos es que nuestro sistema de justicia es deficiente.

Ante el incremento de la ciberdelincuencia se ha aplicado distintos accesos a los datos de los 194 órganos nacionales y de sus socios privados para obtener la actual estadística de apreciación global sobre el incremento de los delitos informáticos respectivos con la covid-19 con el que proyecta una información y enfoque perfecto del panorama de la delincuencia durante la pandemia. La información de la delincuencia internacional de INTERPOL sobre la delincuencia cibernética perpetrada en los meses de abril a mayo del 2020. En 48 países de las 194 naciones han manifestado interés en la investigación y 4 de los 13 socios han proporcionado sus reseñas para el informe. Europa 42%, Asia y Pacífico Sur 19%, Américas 12%, África 17%. El próximo Oriente y Norte de África 10%. (Dirección de la Ciberdelincuencia de Interpol, 2020).

Si bien es cierto en el Perú las amenazas cibernéticas han aumentado con rapidez, aun así, empleando técnicas que dificultan mucho más su descubrimiento, en el primer semestre del 2020, hubo un aumento del 35% de ataques respecto al segundo semestre del 2021 por el igual hecho. Debido a la aparición de la pandemia covid-19 y a los continuos ataques a sus actividades empresariales y personales,

las empresas y los particulares necesitaban aumentar su nivel de protección en materia de ciberseguridad. (Gestión, 2021).

Después de conocer la realidad problemática observada, formulamos el siguiente **problema General: ¿Cuáles fueron las causas que influyeron en el incremento de la delincuencia cibernética a consecuencia del covid-19 en Trujillo 2020-2021?** y los problemas específicos que se plantean son PE1: ¿Qué tipo de modalidades de delincuencia cibernética se dieron con más frecuencia en Trujillo 2020-2021?; PE2: ¿Precisar cuál ha sido el nivel de aumento de delincuencia cibernética a causa del covid-19 Trujillo 2020-2021?; y, PE3:¿Se desarrollaron alternativas para combatir la ciberdelincuencia en Trujillo 2020-2021?.

El presente trabajo de investigación se desarrolla en el ámbito social, ya que es de utilidad para nuestra sociedad, que, a consecuencia del aislamiento social obligatorio, fruto del covid-19, dado por el gobierno, se ha visto expuesta a nuevas modalidades de delincuencia cibernética, mediante llamadas, mensajes de texto, suplantación de identidad, etc.

La justificación teórica, se fundamenta debido a la situación problemática que vincula el incremento de delincuencia cibernética a consecuencia del covid-19 en Trujillo, es importante el efecto de ampliar, profundizar y conocer a través de bases teóricas, leyes, trabajos de investigación de este tema, estadísticas Respecto a la justificación metodológica, realizaremos una investigación de tipo cualitativa en la cual desarrollaremos una descripción de las variables, orientado y basado en el análisis y síntesis sobre nuestra problemática con el fin de recabar información real y contundente para poder compartirla e informar a la población. En base a lo expuesto, se planteó el siguiente **objetivo general**: Determinar las causales del incremento de delincuencia cibernética en tiempos de aislamiento social obligatorio producto del covid-19. Por otro lado, formulamos los siguientes tres **objetivos específicos**:

OE1: Identificar qué tipo de modalidades de delincuencia cibernética se dieron con más frecuencia en Trujillo 2020-2021; OE2: Examinar cuál ha sido el nivel de aumento de delincuencia cibernética a causa del COVID-19 en Trujillo 2020-2021;

y, OE3: Desarrollar las alternativas de solución para los delitos de ciberdelincuencias en Trujillo 2020-2021.

De esta manera se planteó los siguientes supuestos de investigación, el supuesto general es: los principales delitos que se cometieron en la ciudad de Trujillo en los años 2020-2021 fueron los delitos de suplantación de identidad y el delito de fraude informático. Mientras que, los supuestos específicos son: el aislamiento social conduciría un alto incremento de la delincuencia cibernética; o quizá los pobladores de Trujillo no manejan de forma correcta los medios cibernéticos, y como segundo supuesto específico: las autoridades desconocen de la delincuencia cibernética por falta de capacitación en sus entidades donde vienen realizando la investigación de este tipo de delitos informáticos debido a que no tienen una buena capacitación por sus entidades públicas.

II. MARCO TEÓRICO

Antecedentes Internacionales

Dentro de los antecedentes **internacionales**, tenemos a Colombia debido a la presencia de delitos informáticos que fueron en aumento debido al Covid-19.

El autor Cadena (2021), en su artículo titulado "el crecimiento del fraude cibernético en Colombia a lo largo de la pandemia de Covid-19". Concluyó que en Colombia el número de registros aumentó en un 114% entre el 2019 y 2020, estas cifras fueron proporcionadas por el Centro de Cibernética Policial, por el cual el aumento de delitos se debió principalmente a la violación de datos personales, que se llevaron a infringir la información del sitio web para generar un poderoso robo cibernético. (página 24). Así se propagó la pandemia del Covid-19 a nivel mundial, los delincuentes informáticos aprovecharon la situación para realizar robos sistemáticos a través de Internet.

En tal sentido Horianski (2018), concluyó que el cibercrimen fue creado por personas capacitadas en el campo de la informática, lo cual es por ello que en el país se han tipificado diversos delitos relacionados con los delitos cibernéticos, pero las leyes vigentes se consideran insuficientes para combatir los delitos informáticos. (página 63).

Por otra parte, Chocobar (2019), el secretario de gobierno digital de Colombia, señaló que para establecer una cultura de ciberseguridad y defensa digital que evite que muchos usuarios sean vulnerables a posibles ciberataques, es fundamental que Perú invierta en seguridad digital, a nivel de empresas privadas o empresas públicas que inviertan recursos para su seguridad informática. Haciendo referencia a Barboza (2018), nos comenta que el desarrollo de la tecnología ha llevado a la creación de mecanismos que facilitan la utilización de monedas virtuales como bitcoins, criptomonedas y tarjetas de crédito. Como resultado, la cibercriminalidad, uno de los mayores problemas a los que se enfrenta el mundo hoy en día, ha sido posible gracias a estos nuevos modelos de negocio. Uno de los principales problemas del sistema bancario en Colombia es el fraude electrónico con tarjetas de crédito. El phishing es otro método de fraude electrónico en el que se falsifica la información de la tarjeta de crédito del portal al que se intenta acceder. El vishing

es otro método en el que el delito se comete a veces por teléfono haciéndose pasar por personal del banco para engañar a los usuarios y hacerles cometer errores, dándoles así acceso a información confidencial.

Salazar (2019), describe cómo las nuevas herramientas tecnológicas se han inspirado en la evolución para recopilar conocimientos y asegurar los mundos virtuales. Dado que se corre el riesgo de ser víctima de un fraude en línea al realizar cualquier tipo de transacción financiera o pago electrónico, el mundo del comercio en línea plantea riesgos de seguridad. Debido a su uso generalizado en el comercio electrónico, el phishing es la estrategia de persuasión más utilizada por los ciberdelincuentes como medio de operación. Estos incluyen el robo de información personal, a través de los llamados "ladrones de phishing", que atacan a las víctimas por correo electrónico para solicitar datos personales. Entonces, cuando los usuarios ingresan sus correos electrónicos, sin querer brindan datos personales y es así como se convierten en víctimas de un robo sistemático, no solo de información personal sino financiera.

Barboza (2018), En consecuencia, estos nuevos modelos de negocio han creado oportunidades para los delitos informáticos. El fraude electrónico es uno de los mayores problemas en Colombia, y el uso de tarjetas de crédito es uno de los mayores problemas del sistema financiero. El fraude electrónico también se lleva a cabo a través del phishing y phishing, que se comete a través de portales web falsos, intentando acceder a la información de las tarjetas de crédito. A partir de ahora, podemos destacar que ambas naciones, así como América Latina, son las principales víctimas de los nuevos como el phishing, el phishing y las estafas por SMS son ejemplos de ciberdelincuencia. Éstos afectan al sistema financiero al hacer un uso indebido de la información de los usuarios y robar sus identidades. Una de las cuestiones planteadas por los autores es que, dada la dificultad de perseguir los delitos porque es necesario reunir todas las pruebas necesarias para su atribución, no basta con proporcionarles información legal. También es importante invertir en seguridad informática y en la correcta aplicación de las normas.

Acurio (2018), Según el artículo, una de las formas de cometer ciberdelitos es a través de la manipulación para conseguir acciones falsas. El phishing, cuyo objetivo es robar la identidad de los usuarios recopilando información personal a través de medios dudosos como ventanas emergentes o correos electrónicos, es una de las

formas más populares de cometer este delito. En otras palabras, el objetivo del phishing es atacar y engañar a grupos débiles

Antecedentes Nacionales:

Huamán (2020), en su Investigación titulada: “Los Delitos Informáticos en Perú y la Suscripción del Convenio de Budapest”, concluyó que La problemática actual causada por la comisión de delitos informáticos en el Perú está en aumento, con técnicas nuevas como dispositivos electrónicos y un singular de medios tecnológicos por parte de los ciberdelincuentes, posición que hace complicado su tipificación en el ordenamiento jurídico. En el año 2017 en Perú se vio afectado con el uso del ransomware teniendo un 25.1% de aumento; entonces en el 2019, nuestra nación era el tercer país en Latinoamérica más afectado con respecto a los esquemas Spyware; de igual forma en el presente año se mostraron 3012 acusaciones por estafa informática y 247 acusaciones con respecto a la falsificación de identificación en la Divindat; a ello se incorpora lo que es el deficiente presupuesto consignado a contar con tecnología de alta gama para realizar el seguimiento necesario sobre este tipo de delitos (p.121).

Ávalos (2020) argumentó que el Perú debe considerar la importancia de una adecuada profesionalidad fiscal de su servicio civil y la necesidad de establecer elementos normativos contra los delitos informáticos como parte de una política institucional efectiva. En resumen, hay muchos tipos de delitos, pero ninguno de ellos es un problema social, sin embargo, estos deben ser listados, y con la tecnología es posible establecer indicadores para la obtención de evidencia digital para que estos indicadores puedan ser determinantes para la investigación.

Pardo (2018), en su tesis: “Tratamiento jurídico penal de los delitos informáticos contra el patrimonio, distrito judicial de Trujillo, 2018”, concluyó que todos los tipos o formas de delitos informáticos contra la propiedad se introducen descaradamente en el fraude informático, el enfoque del sistema de justicia penal para hacer frente a estos delitos es defectuoso porque dificulta el castigo efectivo de los delincuentes informáticos. Asimismo, el tratamiento legal de los delitos informáticos contra la

propiedad en la particularidad de hurto es viciado, porque la ley peruana no contempla explícitamente los delitos informáticos contra la propiedad y por el tipo de delito, siendo este delito tan manifiesto y ambiguo, el artículo 31 no lo contempla castigar efectivamente la propiedad informática (p.23). Con el adelanto de la tecnología en los actuales años, y más aún con la pandemia del covid-19 se ha visualizado un avance notable de estas herramientas, por tal motivo, ha incrementado la delincuencia cibernética, que poco se conocía hasta la actualidad pero que con lo acontecido ha tomado mayor fuerza, con esto la delincuencia cibernética se ha vuelto una nueva modalidad de robo.

Huayre (2021), en su investigación titulada: “El impacto del cibercrimen en delitos de estafa en el distrito de Lima, 2021”; nombra que “uno de los principales problemas para tener el parecido a la medida del cibercrimen o ciberdelitos puesto que no se tiene mayores datos estadísticos encima de estos delitos. Las empresas no brindan importante información motivo por el cual el temor de los compradores o posibles compradores se rehúsan a su utilización, que en el presente ha aumentado notoriamente, ante todo como resultado de la pandemia por el covid-19, se amplió notablemente el manejo de las redes informatizadas”. (p.24).

Asimismo, Vílchez (2020), nos dijo que la falta de herramientas para investigar y perseguir la ciberdelincuencia, la falta de conocimiento y capacitación de la policía, y el desarrollo de muchas relaciones sociales y económicas a través del uso de herramientas tecnológicas, que resulta evidente la necesidad de tipificar algunos criterios normativos a fin de mejorar su tratamiento en el proceso penal e incorporar nuevas figuras delictivas. En conclusión, una de las principales preocupaciones del sistema de justicia penal es poder subsanar las deficiencias legales del Perú para identificar a los autores de los delitos cibernéticos y los retos asociados a la realización de investigaciones con celeridad.

Schwartz (2020), Debido a los avances tecnológicos que han hecho posible que los ciberdelincuentes perpetren delitos en el ámbito digital, cabe mencionar que los ciberataques provocan pérdidas económicas superiores al 1% del PIB. Según Divincri (2020), el aumento de las transacciones bancarias virtuales ha generado una serie de robos cibernéticos en la región. Puesto que, según la policía, unas de las modalidades más comunes, es que los estafadores envían mensajes a los celulares indicando que su cuenta bancaria ha sido bloqueada, dentro del mismo mensaje envían un link el cual al ingresar te piden los datos y son aprovechados

para vaciar las cuentas bancarias. Cabe enfatizar que la Policía exhorta a tener prevención a estas modalidades, puesto que ahora los robos cibernéticos son los más comunes.

Como lo señala Zevallos (2020), Uno de los retos de la transformación digital de Perú es considerar la posibilidad de una brecha en la seguridad informática. Para ello, es necesario salvaguardar la infraestructura de la información, establecer un comité de ciberseguridad que genere una gestión de riesgos informáticos y fomentar el intercambio de información entre los ciudadanos. y sectores empresariales también es crucial para alertar a las autoridades de ciberataques y es necesario para dar estabilidad informática a los usuarios.

De igual manera Flores (2018) determinó que Perú es el país de América Latina en sufrir más ciberataques, siendo el sector financiero el más afectado. Por lo tanto, lo que más necesita es diseñar mecanismos para enfrentar una gran cantidad de ciberataques, brindando así seguridad de la información.

Categoría 1: Delitos Informáticos.

Subcategorías:

- Criminalidad Informática.
- Dispositivos de Seguridad.
- Uso Inadecuado de la Tecnología.

Se desarrolla el siguiente marco conceptual, identificando a la Categoría 1: Delitos Informáticos; sobre la que Acosta (2020), la define como “Utilizar indebidamente la tecnología para cometer delitos ilegales, invadir la intimidad de la persona o borrar o alterar datos que se hayan descubierto acumulados en dispositivos o servidores.” (P.2). Acerca de las palabras del autor son actos ilegales cometidos por gente mal intencionada, aprovechando las ventajas de la tecnología en beneficio propio y perjudicando a terceros.

Los avances de la tecnología, amparados por la innovación científica han permitido solucionar muchas necesidades del ser humano; no obstante;

Según Choucri (2017), menciona que estas tecnologías pueden ser objeto de abuso para producir condiciones desestabilizadoras, tales como instrumentos de dominación, control y explotación” (p.12) En el transcurso del tiempo, el avance de la tecnología nos ha traído beneficios, así como también perjuicios, en este caso en el aspecto informático, aumentando considerablemente la ciberdelincuencia. Al respecto la ONU (2019), nos menciona que “Las tecnologías de la información y la comunicación abrieron las puertas a los delincuentes, aumentando el volumen y la variedad de los delitos cometidos en y a través de Internet.” (p.5).

Así mismo el autor Villavicencio (2014), expresa que comprendemos a la delincuencia informática como prácticas seductoras que apuntan a burlar las medidas de seguridad, como la irrupción en ordenadores, correo o sistemas de datos utilizando un número de entrada; es decir manifestaba desde estas conductas típicas solamente pueden ser cometidas a través de la tecnología, entonces concluía que no toda infracción puede ser secreto como culpa informática por el solo acto de haber situado la computadora u otro herramienta tecnológica. (p.286)

El autor Agamben (2016), menciona que los dispositivos de seguridad, es que esta mentalidad está conectada con el continuo despliegue de equipos de seguridad nacional como casos de excepción, además este dispositivo captura, dirige, identifica y bloquea gestos, comportamientos, opiniones y palabras de individuos.

(p.22)

Es por ello que Yepes (2018), se dice que el uso inadecuado de la tecnología hoy en día influye demasiado en cuanto a los delitos cibernéticos ya que al realizar mal los manejos de esta pueden hacer cosas que está fuera del marco de la ley como es la falsificación de identidad, clonación de tarjetas, correos basura, extracción, etc. (p.21).

Categoría 2: COVID-19 Subcategorías:

- Hackers Cibernéticos.
- Tiendas Online.
- Información Falsa.

Con respecto a la categoría 2: covid-19 sobre la cual Cimino (2022), señala que la ciberdelincuencia en los últimos años del covid-19 ha producido que los hackers cibernéticos proceden utilizando el miedo a su favor, es decir, aprovechándose de la situación creando en los sitios web información falsa sobre los números de infectados, muertes país por país, pues también se ocultan atreves de las tiendas online para de esa manera encriptar un sin número de virus y códigos que les permite apropiarse de las reseñas bancarias en el momento que realizan la validación del carrito.

Según american thoracic society (2020), argumentan que el covid-19 de alguna manera es la enfermedad del coronavirus motivo por el cual obedecen al nuevo virus SARS - CoV2 pues esta genera una plaga aguda con señales respiratorias.

El reciente virus es diverso de los que generan el SARS (síntomatología pulmonar aguzado rígido) o el MERS (síntomatología pulmonar del medio oriente) (p 18)

Así mismo el autor Vargas (2018), señala que los hackers cibernéticos son aquellas personas especializadas en sistemas informáticos con un excelente manejo de las computadoras que realizan daños al unirse a cualquier red sin autorización de nadie y lo hace con motivos maliciosos. (P.20)

Al respecto Laudon (2018), Las tiendas en línea se definen como "el uso de Internet, la web, las aplicaciones móviles y los navegadores que funcionan en dispositivos para realizar transacciones comerciales, lo que permite habilitarlas digitalmente entre organizaciones y particulares". (p. 50)

al referirnos a información falsa, citamos a la Unesco (2021), quien define lo siguiente: "cualquier información que haya sido creada y difundida intencionadamente con el fin de engañar, persuadir o convencer a un tercero para que crea una mentira o impugne verdades verificables."

Según González (2020), "La pandemia del covid-19 tiene un impacto global, al igual que la actuación de los ciberdelincuentes aprovechándose de la situación actual, con un importante resurgimiento de sus operaciones en varios países del mundo" por ello explicamos que, así como cómo avanza la epidemia, aumenta el cibercrimen en todos los países ya que en la actualidad existen tanto grandes como

pequeñas empresas de delincuencias organizadas siendo la ciberdelincuencia un sector ilegal que operan al fuera del margen de la ley. (p.11)

De esta manera Iglesias (2020), nos señala que “La crisis presente puede ser un terreno fértil para que acostumbrados hechos astutos que se extienden por la red se reciban más perjudicados, ya que gran cantidad de la asociación está más tiempo enlazada de lo acostumbrado”, a raíz de la pandemia del covid-19 y dada la nueva modalidad virtual muchas personas se encuentran mucho más tiempo conectados a una red de internet y de esa mera nos exponemos a los riesgos de que los delincuentes accedan de manera más rápida a nuestros datos.(p.23)

Asimismo, Schwartz (2020), Manifiesta que la crisis ocasionada a comienzo de 2020 por la pandemia del covid-19 acomodo al margen nuestra subordinación de una base fundamental, puesto que nuestra vida diaria gira alrededor de actividades progresivamente exploradas, es así entonces que esto nos aproxima a estar más próximos a amenazas cibernéticas. Estas se realizan en la actualidad a través de tecnologías dactilares, resaltando la diplomacia de ciberseguridad entendemos que son primordiales para salvaguardar los tributos de los civiles en la esfera digital.

(p.1).

III. METODOLOGÍA

3.1. Tipo y diseño de investigación

3.1.1. Tipo

La presente investigación se desarrolló en forma cualitativo - básica. Kemmis y Mc Taggart (2020), puntualizan a la investigación básica como “el proceso de reflexionar sobre un tema determinado en el que le gustaría mejorar su práctica o comprensión personal. Por lo tanto, los implementadores realizan investigaciones para definir claramente el inconveniente y especificar un plan de acción. Luego se lleva a cabo una valoración para verificar e instituir la efectividad de la acción tomada”.

3.1.2. Diseño

La investigación presento un conocido diseño como teoría fundamentada. La teoría de la base procesal es el método de análisis de datos de comparación constante mediante el cual el investigador sistematiza y analiza los datos simultáneamente para el desarrollo progresivo de ideas teóricas estrechamente relacionadas con los datos, estableciendo cuatro pasos: comparar los problemas aplicables a cada uno, integrar los tipos y sus propiedades, delinear la teoría y su ortografía.

Strauss, et al. (1967), esta metodología fue presentada en la publicación de su libro por lo que este diseño conocido como teoría fundamentada, se basa únicamente en el análisis de datos, los cuales obtendremos a través de la información que proporcionará nuestra investigación.

Finalmente, para el análisis de datos de este diseño, se realizó dos momentos, momento relacional y descriptivo, de cada uno con su propia particularidad de codificación. El primer es descriptivo, se logra a través de un proceso de codificación abierta, es decir, asignando etiquetas para describir los contenidos de dichos segmentos, buscando definir conceptos, atributos y dimensiones en los datos. El segundo relacional, desarrollado a través de axial y procesos de codificación selectiva, primera codificación 16, axial, permite describir datos a nivel de organización segunda codificación y

organización selectiva, permitiendo el proceso de aparición de categorías en un diagrama de un esquema conceptual.

3.2. Categorías, subcategorías y matriz de categorización

Categorías

Al referirnos a Categorías, Seiffert (1997), la define como una abstracción de tres características y atributos de las cosas y fenómenos, ayudando a organizar la visión de la realidad. Es decir, es imposible entender qué es una categoría sin referirse a palabras y objetos del mundo: encontramos objetos en el mundo y les asignamos palabras para referirnos a ellos y representarlos.

Categoría 1: Delitos Informáticos

Subcategorías:

- Criminalidad Informática.
- Dispositivos de Seguridad.
- Uso Inadecuado de la Tecnología. **Categoría 2: COVID-19**

Subcategorías:

- Hackers Cibernéticos.
- Tiendas Online.
- Información Falsa.

3.3. Escenario de estudio.

El escenario de estudio fue en las comisarías y las fiscalías de la ciudad de Trujillo, con la finalidad de conocer cuáles fueron las causas que influyeron en el incremento de la delincuencia cibernética a consecuencia del covid-19 en Trujillo 2021-2022.

3.4. Participantes

Para esta investigación cualitativa se consideró contar como participantes a tres representantes de la policía nacional del Perú y tres representantes del Ministerio Público con conocimiento en derecho penal y competencia en ciberdelincuencia, para de esa manera precisar cuál ha sido el nivel de aumento de delincuencia cibernética a causa del covid-19, y es así como los participantes son los subordinados que son sustanciales en un trabajo de investigación ya que ellos aportan gran parte de información sustancial para poder dar desarrollo a los objetivos establecidos.

3.5. Técnicas e instrumentos de recolección de datos.

3.5.1. Técnicas

Como técnica del trabajo de investigación se realizó entrevistas y el análisis documental de las comisarías de Trujillo y las fiscalías de Trujillo, es de esa manera que según la definición dada Según Rojas (2016), "Este es un procedimiento típico, validado por hechos, a menudo orientado a la adquisición y transformación de información útil para resolver problemas de conocimiento en las ciencias, cada uno de los cuales prevé el uso de un motor de aplicación". (pág. 278).

3.5.2. Instrumentos

Como instrumentos se empleó la aplicación de entrevistas y el análisis documental de las comisarías de Trujillo y las fiscalías de la ciudad de Trujillo por ende Según los autores: Hernández, et al. (2014) el instrumento para un enfoque cualitativo, es un recurso que se utiliza para registrar la búsqueda o datos sobre las variables. Motivo por el cual se realizó una entrevista y un análisis documental, con la finalidad de obtener resultados válidos para la investigación.

Así mismo, Benadiba, et al. (2020) refieren que la entrevista es un diálogo sistematizado con el propósito de recolectar, rescatar y registrar experiencias de vida almacenadas en la memoria de las personas. Es un ambiente en la

que, a través del lenguaje, el entrevistado cuenta su historia y el entrevistador le hace preguntas sobre evento, situación (p.48).

3.6. Procedimiento

El proceso de investigación comenzó con la identificación del problema y la descripción de las categorías y subcategorías. que desarrolla sus objetivos y presunciones. Para estos últimos, contrastan un abanico de teorías y las respuestas proporcionadas por expertos. Los resultados fueron presentados y discutidos hasta llegar a las recomendaciones y conclusiones pertinentes.

3.7. Rigor científico

Según Ratcliffe et al. (2011), se basa en teorías de reduccionismo y universalidad y enfatiza el pensamiento analítico. Una de las críticas a la investigación cualitativa tiene que ver con el rigor de la ciencia, hasta el punto de afirmar que el rigor no es un signo de naturalismo, por lo que se enfatiza en el rigor del modelo del naturalismo.

3.8. Método de análisis de la información.

Las entrevistas cualitativas, se realizó utilizando herramientas de recolección de datos para probar hipótesis utilizando preguntas incluidas en la guía de la entrevista. Dado que las respuestas de las entrevistas, se estudiarán individualmente, validarán las hipótesis formuladas en relación con nuestros objetivos, el análisis de contenido será una de las técnicas de análisis de datos empleadas.

3.8.1. Método comparativo

Arias (2020), el método comparativo es para refutar hipótesis y teoría, utiliza un procedimiento similar al método científico para comparar por lo que persigue utilizar la ciencia para afirmar los argumentos y estudiar similitudes y diferencias.

3.8.2 Método analítico

Según Martínez (2018), este método se especificó para analizar documentos sobre temas de investigación de modo que se puedan extraer los elementos más importantes relevantes para el objeto de investigación.

3.8.3 Método inductivo

Según Abreu (2014), la inducción propone un razonamiento ascendente que fluye de lo específico o individual a lo general. La premisa de la inducción es una reflexión centrada en el propósito. Así la inducción es un resultado lógico, metodológico de la aplicación del derecho comparado. Según el autor Torres (2019), nos explica que el método inductivo este consiste en generalizaciones de hechos, situaciones o hábitos observados en un caso concreto, en donde se puede facilitar al investigador y de esa manera contactar al sujeto de estudio. Siendo así que el camino que va de mayor cantidad de los objetos a menor unidad de conceptos. (p.5)

3.9 Aspectos éticos

Con respecto a los criterios que se tomaron en cuenta por el investigador, que garantizan la calidad de redacción con la que fue realizada la investigación, cumpliendo con las reglas y normas que requiere el formato de la universidad, se utilizó las correspondientes normas APA (American Psychological Asociación), en su séptima versión, consignando citas, autorías y bibliografía correspondiente, de igual manera se siguieron los lineamientos establecidos por la Universidad César Vallejo. Respecto en esta investigación las técnicas y los datos utilizados son las cualitativa- básica, requerimos de 2 instrumentos, tales como entrevista que se llevó a cabo a través de entrevistas verbales y también un análisis documentario, estos se realizaron con el fin de delimitar adecuadamente el problema de investigación de este trabajo en relación a las dos categorías establecidas en este proyecto; el Incremento de Delincuencia Cibernética y pandemia COVID.

IV. RESULTADOS Y DISCUSIÓN

4.1 RESULTADOS

A través del siguiente instrumento de guía el investigador analizo entrevistas seleccionadas para determinar las causales del incremento de delincuencia cibernética en tiempos de covid-19. Para el desarrollo de este trabajo de investigación se realizaron entrevistas a expertos en el campo de las ciencias penales conocedores de los delitos informáticos. Los entrevistados fueron tres miembros del ministerio público de la ciudad de Trujillo y tres miembros del departamento de policía de Trujillo; es importante señalar que también se contó con su ayuda para la recopilación de datos e información a fin de cumplir con el objetivo específico número 2 de la investigación. Los informes, que son puestos a disposición por la Policía Nacional del Perú, corresponden a denuncias que fueron presentadas ante la división de delitos de alta tecnología entre enero de 2020 y diciembre de 2021 con base en estos informes, se elaboraron cuadros con el objetivo de conocer y evaluar mejor el registro de casos relacionados con el crecimiento anual de casos relacionados con delitos informáticos y el tratamiento dado el sistema de justicia penal y el sistema de registro de denuncias de investigación criminal de la policía nacional peruana, así como el incremento anual de casos relacionados con delitos informáticos.

Con respecto al análisis del objetivo específico N° 01, que se refiere a: Identificar qué tipo de modalidades de delincuencia cibernética se dieron con más frecuencia en Trujillo 2020-2021.

Se han realizado las siguientes tablas.

TABLA 1:

Incidencia de los delitos en materia de ciberdelincuencia en la ciudad de Trujillo en los años 2020-2021.

PREGUNTA 1: ¿Cuáles son los delitos en materia de ciberdelincuencia que tuvieron más incidencia en la ciudad de Trujillo entre el año 2020-2021?

E1

E2

E3

Los delitos con mayor incidencia en el ministerio publico fueron los delitos de suplantación de identidad con un porcentaje de del 78% de aumento entre los años del 2020-2021 pero también aumentaron los delitos de fraude informático con un porcentaje de 38%.

El delito con mayor incidencia en el año 2020 en la comisaria del alambre fue el delito de suplantación de identidad y también se produjo algunos delitos informáticos como robos a través de estafas cibernéticas a consecuencia de la nuevas plataformas digitales en la cual los afectados de la estafa realizan sus pagos por medios de aplicativos digitales como yape , plim y también a través de trasferencias bancarias e interbancarias que se maximizo en pandemia por las restricciones del gobierno central. En el año 2021 las incidencias de delitos informáticos

La suplantación de identidad fue el delito con más reincidencia en la ciudad de Trujillo en los años 2020 hasta el 2021 que aumento en la comisaria de Ayacucho acercándose varias personas a presentar su denuncia correspondiente por el delito de suplantación de identidad
Con la nueva ley de delitos informáticos ley número 30096.

aumentaron de gran manera por que ahora se ha producido mayor aumento de delitos informáticos como se apreciar en los informes anuales que presenta la comisaria.

E 4	E5	E6
Las denuncias recibidas en la comisaria del Alambre muestran que el delito de suplantación de identidad tiene un mayor porcentaje sobre todos los delitos de ciberdelincuencia en el año 2020 hasta el 2021.	Las denuncias con mayor incidencia han sido las de suplantación de identidad y también la de estafas cibernéticas como el gota a gota.	En la comisaria de la noria las denuncias más recurrentes fueron las de suplantación de identidad ya que fue la que más afecto a la población en la época de covid-19 debido a que las personas se registraban para cobrar su bono yanapay y resultaron estafadas.

INTERPRETACIÓN: Los 6 especialistas han coincidido en que delito informático con mayor incidencia en los años 2020 hasta el 2021, es el delito de suplantación de identidad con un porcentaje de 78% de aumento en los mencionados años. En consecuencia, los 6 especialistas han convenido que ante la omisión de las entidades públicas por no contar con los recursos necesarios para combatir la delincuencia cibernética es debido a ello el aumento de la cifra anual, por lo mismo se necesita mucha capacitación para el personal y también implementación de nuevos mecanismos para combatir la ciberdelincuencia.

Fuente 1: Entrevistas aplicadas a especialistas

Tabla 2:

Acciones para combatir la ciberdelincuencia en la ciudad de Trujillo en los años 2020-2021

PREGUNTA 2: ¿Qué acciones se realizaron para combatir la ciberdelincuencia en la ciudad de Trujillo en los años 2020-2021?

E1	E2	E3
Se tomaron medidas preventivas en la cual se informó mediante la plataforma digital del Ministerio público a la sociedad a través de Facebook las nuevas modalidades de estafas de los delincuentes que utilizan para realizar la suplantación de identidad y también el robo de información personal, causando múltiples desfalcos económico a diferentes personas en los años 2020 hasta el 2021.	Se opto por múltiples opciones para poder contrarrestar las nuevas modalidades de la delincuencia cibernética la cual se están poniendo en prácticas a diario capacitando al personal encargado del área de sistemas de la policía Para la identificación de los softwares maliciosos de los hackers, los antivirus y se realiza un análisis continuo de los archivos. Estos programas se pueden instalar en computadoras de escritorio, laptops, Tablet y celulares, y lo defienden de	Se recomienda a la población no utilizar enlaces que provienen de un correo extraño, en el caso de navegadores realizar la navegación un buscador reconocido como Google crome para verificar la dirección de donde estamos ingresando nuestros datos y así no ser víctima de estafas cibernéticas a través de dispositivos informáticos , agregar signos de puntuación asteriscos números a las contraseñas que utilizamos a diario esa información la esparcimos todo el años

	“gusanos informáticos”, “troyanos” y “virus”, entre otros.	2020 y 2021 para que disminuya los delitos informáticos.
--	--	--

E4	E5	E6
<p>Tomamos la iniciativa de brindar charlas informativas con relación a los delitos informáticos para educar a la población a no caer en el error de ingresar a paginas desconocidas o ser víctima de suplantación de identidad por ello también se les comunico estar atento a los enunciados del gobierno mediante radio y televisión.</p>	<p>Con supervisión de mi comandante de la comisaria de bellavista fuimos a distintos puntos para ayudar a la gente a cobrar sus respectivos bonos y evitar que sean víctimas de la delincuencia cibernética.</p>	<p>Se realizo una guía para las personas que desconocen el uso adecuado de la tecnología y así evitar una mayor propagación de los ciberdelitos.</p>

INTERPRETACIÓN: Los 6 especialistas han señalado que realizaron diversos métodos para combatir la delincuencia cibernética en los cuales no fueron efectivos en los años 2020 y 2021 aumentando la cifra de delincuencia en un 78% en la cuales muchas personas fueron afectadas con las nuevas modalidades de ciberdelincuencia desfalcando sus cuentas bancarias con el delito de suplantación de identidad y también con los fraudes como las estafas con los aplicativos de envíos de dinero a través de yape y plim y trasferencias bancarias.

Fuente 2: Entrevistas aplicadas a especialistas

Tabla 2:

Roles de las entidades bancarias para buscar combatir la ciberdelincuencia.

PREGUNTA N° 03: ¿Cuál fue el rol de las entidades bancarias/financieras para la búsqueda de soluciones en los delitos de ciberdelincuencia?

E1	E2	E3
Las entidades financieras y los bancos ofrecieron a los usuarios mecanismos de seguridad como los tokens, claves temporales, parametrización de montos en las transacciones para evitar algún tipo de robo sistemático o suplantación de identidad por parte de los delincuentes cibernéticos.	Los bancos usan el mecanismo de mensaje de texto para poder advertir a sus clientes de cualquier intento de suplantación de identidad o transacciones que no se generaron por el cliente eso ayudado a disminuir los delitos cibernéticos.	Muchas entidades bancarias usaron el mecanismo del correo electrónico y vinculación a su dispositivo móvil, lo cual ha favorecido a usuarios, porque he evitado muchos robos sistemáticos, ya que, con dicho correo, podíamos conocer qué tipo de movimientos se están alertando y así poder llamar al banco y evitar robos.
E4	E5	E6
Las entidades bancarias desarrollaron aplicativos oficiales como (BCP móvil	Los bancos usaron el mecanismo de alertar a la población mediante mensajes	Todos los bancos, optaron por mejorar la seguridad en sus plataformas digitales,

tunqui billetera digital, etc.) para brindar seguridad al momento de realizar operaciones bancarias, a su vez también atendía algunos pequeños imperfectos en el aplicativo para una mejor experiencia. de texto, manifestando que ellos no solicitan información personal a los usuarios, ya que cualquier trámite es de manera personal y portando el DNI, dicha información ha servido para evitar delitos de suplantación de identidad.

INTERPRETACIÓN: De los resultados obtenidos por los 6 especialistas, 3 han coincidido en que la solución de los bancos ante los ciberdelitos, fue alertar a la población mediante mensajes de texto. Por otro lado, los otros 3 especialistas coinciden en que los bancos solucionaron el incremento de los ciberdelitos, mejorando la seguridad en sus plataformas digitales. Debido a esto la seguridad para los usuarios ha mejorado considerablemente respecto a los delitos informáticos relacionado con los bancos y financieras.

Fuente 3: Entrevistas aplicadas a especialistas

Tabla 4:

Identificación de autores de los delitos cibernéticos en Trujillo 2020-2021

PREGUNTA N° 04: ¿Qué tan difícil han sido identificar a los autores de los delitos de ciberdelincuencia en la ciudad de Trujillo 2020-2021?

E1	E2	E3
Ha sido difícil para el ministerio publico combatir con los delincuentes cibernéticos, ya que no contamos con herramientas tecnológicas que favorezcan las investigaciones eso no ha dificultado mucho la identificación de los infractores que usan las redes para delinquir.	La identificación de los delincuentes cibernéticos es muy difícil de lograr ya que lastimosamente la PNP no cuenta con herramientas del mismo nivel que los hackers, por ende, solo nos enfocamos en rastrear las llamadas, cuando intentan suplantar la identidad de alguna persona.	Es muy penoso saber que no contamos con las herramientas necesarias para combatir la delincuencia digital, esto nos ha limitado para ayudar a la población a solucionar los conflictos relacionados con la tecnología.
E4	E5	E6
Muchas veces es difícil identificar a los autores de los ciberdelitos, ya que en primer lugar no se cuenta con las mismas herramientas tecnológicas necesarias y a	Es difícil para nosotros como policías no saber cómo actuar frente a esos delitos tecnológicos que cada día avanzan y superan expectativas e identificar a	La identificación de los delincuentes cibernéticos es un trabajo difícil, porque no se cuenta con un presupuesto destinado a mejorar nuestra tecnología,

su vez el personal no está capacitado para quienes delinquen es una tarea casi para con ello poder solucionar los poder realizar las investigaciones imposible porque no se cuenta con las problemas de la sociedad, sin embargo, correspondientes en el ámbito herramientas necesarias para con las pocas herramientas que tenemos, tecnológico. combatirlos. brindamos el mejor apoyo a la población, algunas veces satisfactorias, por que logramos identificar y capturar al delincuente y en otras seguimos en etapa de investigación.

INTERPRETACIÓN: De los resultados 6 especialistas, todos han coincidido en que es difícil lograr identificar a los autores de los delitos cibernéticos por falta de herramientas tecnológicas, las cuales favorecerían mucho en las investigaciones correspondientes. Sin embargo, al no contar con dichas herramientas (software, hardware, dispositivos y maquinas), se les hace difícil el esclarecimiento de los autores involucrados en el delito informático.

Fuente 4: Entrevistas aplicadas a especialistas

Tabla 5:

Delitos informáticos en etapa de juzgamiento en la actualidad en Trujillo 2020-2021.

PREGUNTA N° 05: ¿En la actualidad cuantos casos de delitos informáticos se encuentran en una etapa de juzgamiento en la ciudad de Trujillo en los años 2020-2021?

E1	E2	E3
Por ahora si tenemos casos en etapa de juzgamiento dentro de la fiscalía, pero la mayoría están en diligencia preliminares y algunas en investigación preparatoria, por la falta de herramientas tecnológicas es que no se pueden formalizar muchas denuncias.	En la comisaria tenemos denuncia por delitos informáticos, pero no se puede hacer mucho ya que no se cuenta con las herramientas necesarias, sin embargo, nosotros derivamos a la Divindat, para que puedan cooperar en las investigaciones para determinar la culpabilidad del imputado.	Desde el ministerio público, tratamos de identificar a los delincuentes que se ocultan en las redes sociales, haciendo uso de las pocas herramientas tecnológicas que posee la PNP para continuar con las investigaciones necesarias, por ello es difícil llegar a la etapa de juzgamiento.
E4	E5	E6
Por el momento el ministerio público no ha informado en qué estado se encuentran dichas denuncias ya que están en etapa de investigación preparatoria es decir	En nuestra comisaria hemos recibido denuncias sobre delitos informáticos, los cuales comunicamos al MP, para las investigaciones correspondientes, sin	Conforme la ley 30096 se debe sancionar a los autores que cometen delitos informáticos, sin embargo, en muchos casos aún no se identifican a los autores

sigue en investigaciones para determinar embargo, no se tiene noticias aun de que lo que hace imposible sancionarlos por a los autores y así poder sancionarlos. dichos casos están en etapa de ellos es importante las herramientas tecnológicas para acelerar las juzgamiento. investigaciones.

INTERPRETACIÓN: De los 6 especialistas, el 02, 04 y 05, coinciden en que las denuncias por delitos cibernéticos aún se encuentran en etapa de investigación, sin embargo, los especialistas 01, 03 y 06 manifiestan que las denuncias por delitos informáticos se encuentran archivadas, en proceso, y terminación anticipada haciendo un total de 2000 denuncias. De estas, un 55% (1050) han sido archivadas y un 45% (950) que se encuentran en proceso de investigación.

Fuente 5: Entrevistas aplicadas a especialistas

Tabla 6:

Procedimientos para la investigación de la ciberdelincuencia.

PREGUNTA N° 06: ¿Qué mecanismos o procedimientos faltan para una adecuada investigación en los delitos de ciberdelincuencia?

E1	E2	E3
El gobierno debe destinar un fondo para la compra de herramientas tecnológicas, para así nosotros conforme a nuestra función investigadora usar las	Se necesita capacitar a los miembros de la PNP, así como también al propio MP, para que tengan conocimientos actuales de cómo combatir la delincuencia	Necesitamos la implementación de los softwares actualizados para rastrear llamadas o mensajes de los facinerosos y así combatirlos, además de ello se debe

herramientas del mismo nivel tecnológico que los infractores y combatir la delincuencia cibernética que está avanzando rápidamente en nuestro país, ello ayudara a mucho a reducir las estafas y los delitos por suplantación de identidad entre otros.

cibernética desde todos los sus ángulos, y nos vemos limitados en conocimientos digitales, también debemos contar con tecnología de punta, para realizar las investigaciones de manera eficaz.

implementar una sede especial para delitos informáticos muy aparte de la sede que se ubica en Lima. Ya que, si todas las ciudades contáramos con dicha entidad, fuera más fácil adquirir herramientas tecnológicas, por la misma demanda de la gente al realizar las denuncias relacionadas con los delitos cibernéticos.

E4

E5

E6

Para realizar una adecuada investigación, debemos contar únicamente con herramientas tecnológicas mucho más avanzado que los delincuentes, para con ello combatirlos, porque sin las herramientas necesarias no se puede hacer mucho para identificar a los delincuentes ni mucho menos para continuar con las investigaciones correspondientes y esto dificulta la tarea de la PNP.

Para nosotros realizar investigaciones contra los delitos cibernéticos, debemos adquirir herramientas tecnológicas que favorezcan el trabajo, seguido a ello necesitamos capacitaciones respecto a la tecnología, por que como sabemos este avanza de manera desmesurada y sin una capacitación de las novedades actuales, nos veríamos limitados para actuar contra estos delitos.

Falta inversión en tecnología, luego de ello capacitarnos a quienes llevaremos las investigaciones en este caso el Ministerio Publico, para poder realizar un trabajo adecuado, a su vez realizar pequeñas charlas a la población para que conozcan un poco más y educarse con la tecnología que hoy en día es inevitable contar con ella.

INTERPRETACIÓN: De los resultados obtenidos los 6 especialistas, coincidieron que para una mayor investigación en los delitos cibernéticos es necesario contar con las herramientas tecnológicas de primer nivel y a su vez capacitaciones constantes para poder continuar las investigaciones de manera correcta y satisfactoria.

Fuente 6: Entrevistas aplicadas a especialistas.

RESULTADOS OBJETIVO ESPECIFICO 01: Se identificó que tipos de modalidades de delincuencia cibernética se dieron con más frecuencia en Trujillo, de acuerdo a las entrevista aplicadas a los representante del ministerio público y a los oficiales de la policía nacional, se obtuvo resultado que los delitos realizados con más frecuencia son robo de identidad, estafa piramidal, estafa de créditos bancarios, delito de hacker de información de cuentas bancarias y suplantación de identidad por redes sociales de los cuales se produce por el mal manejo de la tecnología. Por la falta de presupuesto y apoyo de sus autoridades es muy difícil para las instituciones encargadas en las investigaciones detectar las nuevas modalidades de ciberdelitos. Así mismo se determinó que el delito de FRAUDE INFORMÁTICO tiene mayor incidencia en la ciudad de Trujillo durante la pandemia del covid-19 entre los años 2020 hasta el 2021 por eso es de vital importancia contar con el apoyo del gobierno actual para fortalecer las entidades públicas como las comisarias y las fiscalías quienes son las encargadas de realizar las investigaciones.

Con respecto al análisis del **objetivo específico N° 02 el cual es:**

“Precisar cuál ha sido el nivel de aumento de delincuencia cibernética a causa del COVID-19 en Trujillo 2020-2021”.

Tabla 7:

Nivel de aumento de los delitos cibernéticos entre los años 2020-2021

Análisis Documental

Año	Meses	Tipos de delito	Cantidad de denuncias	Entidad	Aportes
2020	Enero-diciembre	fraude informático de suplantación identidad	186	Comisaría Alambre	Recolección de datos para seguir el debido proceso.
		fraude informático abuso de mecanismos y dispositivos informáticos	140	Comisaría de Ayacucho	Toma declaraciones e intervención policial.
		fraude informático abuso de mecanismos y dispositivos informáticos	145	Comisaria de la Noria	Recolección de medios probatorios para la formalización de denuncia.
		fraude informático de suplantación identidad	133	Comisaria de Bellavista	Intervención policial y toma de declaraciones.
		fraude informático abuso de mecanismos y	165	Ministerio Publico de la Libertad	Formulación de la investigación preparatoria.

		dispositivos informáticos			
		fraude informático abuso de mecanismos y dispositivos informáticos	113	Ministerio Publico mixta de la Esperanza	Formulación de la investigación preparatoria.
		fraude informático de suplantación identidad	125	Ministerio Publico del Porvenir	Formulación de la investigación preparatoria.
2021	ENERO - DICIEMBRE	fraude informático de suplantación identidad	180	Comisaría Alambre	Recolección de datos para seguir el debido proceso
		fraude informático abuso de mecanismos y dispositivos	156	Comisaría de Ayacucho	Toma declaraciones e intervención policial.
		fraude informático abuso de mecanismos dispositivos informáticos	134	Comisaria de la Noria	Recolección de medios probatorios para la formalización de denuncia.
			167		Intervención policial y toma de declaraciones.

fraude informático de suplantación identidad		Comisaria de Bellavista	
	289		Formulación de la investigación preparatoria.
fraude informático abuso de mecanismos y dispositivos informáticos		Ministerio Publico de la Libertad	
	234		Formulación de la investigación preparatoria.
fraude informático de suplantación identidad		Ministerio Publico mixta de la Esperanza	
	256		Formulación de la investigación preparatoria.
fraude informático abuso de mecanismos y dispositivos informáticos		Ministerio Publico del Porvenir	

INTERPRETACIÓN: Las denuncias por delitos informáticos de 2020 a 2021 se muestran en el cuadro. Teniendo en cuenta que a partir del 2019 nos adheriremos al Convenio de Budapest de acuerdo a la Ley N.º 30096 y su revisión, se podrá observar un crecimiento paulatino durante los dos últimos años. Esto nos lleva a señalar que tanto el robo de identidad como el fraude informático tienen mayores tasas de incidencia que otros delitos, teniendo el fraude informático un porcentaje del 78,2% del total de casos. Fuente de elaboración propia de autores.

RESULTADOS OBJETIVO ESPECIFICO 02: Tras el análisis de los documentos, se pudo comprobar fácilmente que existían 968 denuncias por delitos informáticos. Debido a la falta de tipificación del hecho ilícito en los métodos que los ciberdelincuentes emplean con frecuencia para estafar a las personas de tipos delictivos concretos que se cometen con mayor frecuencia en la red, se desprende del incremento anual de las denuncias que, a pesar de los esfuerzos de las fiscalías y los funcionarios judiciales, no son capaces de asignar correctamente las responsabilidades. Esto nos permitió ver la falta de cultura informática, que es un elemento crucial para combatir el aumento de los delitos informáticos. Debido a ello, existieron diversas denuncias formuladas, denuncias pendientes de resolución y denuncias que culminaron en el archivo, de acuerdo al número de denuncias por delitos informáticos brindadas por la Policía Nacional del Perú durante los años 2020 y 2021. Para sacar una conclusión, es importante señalar la falta de conocimiento sobre los alcances de los delitos informáticos, lo cual nos permite entender cómo manejar situaciones particulares y además brinda seguridad al usuario al utilizar herramientas tecnológicas para definir las leyes en base a la realidad social de nuestra nación.

Con respecto al objetivo específico N° 03, que se refiere a desarrollar las alternativas de solución para los delitos de ciberdelincuencias en Trujillo 2020-2021.

Con relación a las respuestas obtenidas por los especialistas entrevistados, tenemos:

Tabla 8:

Necesidad de una fiscalía especializada en ciberdelincuencia.

PREGUNTA 07: ¿Resultaría necesario la creación de una fiscalía especializada en ciberdelincuencia en la ciudad de Trujillo?

¿por qué?		
E1	E2	E3
Claro que si resultaría necesario una sede especializada en delitos informáticos, para que pueda favorecer en el esclarecimiento de los hechos delictivos de índole informática y con ayuda de las herramientas necesarias y nueva tecnología se podría dar resultados positivos en la identificación de los autores de estos delitos.	La creación de una sede especializada en delitos informáticos en la ciudad de Trujillo ayudaría a descentralizar la carga que tiene en la DIVINDAT ubicada en la ciudad de Lima, sería de mucha ayuda que gente especializada en el tema informático colabore con las investigaciones para determinar quién es el autor de los delitos en la ciudad de Trujillo.	Sería de gran ayuda contar con una sede especializada en delitos informáticos en la ciudad de Trujillo, cabe resaltar que con la suscripción del convenio de Budapest se puso a disposición la unidad fiscal especializada en ciberdelincuencia, esto de alguna manera ha favorecido en la resolución de algunos delitos informáticos, ya que se cuenta con personal capacitado en tecnología.

E4	E5	E6
<p>Si resultaría muy necesaria la creación de una sede fiscal como en la capital que tiene una fiscalía especializada en delitos informáticos en Lima centro donde se pueden tener mayor enfoque al momento de llevar ese tipo de casos ya que en la actualidad en la ciudad de Trujillo no tenemos las herramientas necesarias para combatir los ese tipo de ilícitos por eso la mayoría de casos que logramos formalizar siempre no llegan a juzgamiento y llegan a un sobreseimiento o al archivo.</p>	<p>Estoy de acuerdo que el ministerio público pueda tener mayor conocimiento de los ciberdelitos por eso sería factible la creación de una fiscalía en la ciudad para así facilitarnos nuestro trabajo como servidores públicos y como la policía realizamos nuestras labores a diario pero vemos que no son suficientes la tecnológica que tenemos en nuestra dependencia policial para combatir a los delincuentes que día a día se ingenian con muchas más tecnología para cometer sus delitos y así quedar impunes .</p>	<p>La verdad que sería grandioso que los representantes del ministerio público puedan tener una sede en el departamento de Libertad y no solo en Lima como la tienen ahora debido a que en todo el Perú se cometen delitos informáticos no solo en Lima por eso debería la fiscal de nación comprometerse con la creación de fiscalías especializada en ciberdelitos para poder así combatir el crimen organizado que está afectando diariamente a la población de nuestra región.</p>

INTERPRETACIÓN: Conforme a los 6 especialistas entrevistados , todos coinciden en que debería crearse una fiscalía corporativa especializada como tienen en Lima en delitos informáticos , aquí en la ciudad de Trujillo ya que al instaurarse dicha sede, ayudara a obtener herramientas sofisticadas para el desarrollo de las investigaciones así mismo se podrá capacitar al personal necesario para que puedan desarrollar de manera satisfactoria su trabajo relacionado con los delitos informáticos, de lo contrario toda investigación se quedara en esta misma etapa, sin poder brindar soluciones satisfactorias a la población.

Tabla 9:

Capacitaciones y participación de los representantes de entidades públicas en los años 2020-2021 Trujillo.

PREGUNTA 08: ¿Qué capacitaciones a participado o en que capacitaciones a participado en relación a los delitos informáticos en el año 2020-2021 en la ciudad de Trujillo?

E1	E2	E3
En ninguna capacitación por el momento la fiscalía no ha capacitado a su personal encargado de estos ilícitos, pero por mi parte si tengo conocimiento de algunas cosas sobre la ciberdelincuencia ya que estas modalidades de delinquir están a la orden del día por lo mismo tenemos que	Por el momento en ninguna capacitación debido a que la policía nacional del Perú no tiene capacitaciones frecuentemente y sobre todo no tiene mucho conocimiento de los delitos informáticos por eso pedimos a nuestra institución que nos pueda capacitar para poder tener un	Solo nos brindan folletos de las nuevas tecnologías que utilizan los ciberdelincuentes, pero no participe en ninguna capacitación porque mi institución no las brinda limitando así nuestro trabajo a diario ya que a veces se puede hacer muchas más cosas, pero con

<p>estar nosotros capacitados como sugerencia se pueden recomendar, pero por si la fiscalía no está brindando esa herramienta.</p>	<p>mayor conocimiento de las nuevas modalidades delictivas que existen actualmente y así estar a la vanguardia porque si no estaremos combatiendo el crimen con tecnología desfasada y no actualizada como se requiere en estos tiempos.</p>	<p>la tecnología que tenemos no se puede hacer nada solamente realizar la investigación pertinente y la denuncia por parte del agraviado nada más.</p>
--	--	--

E4	E5	E6
<p>No, por el momento no tengo conocimiento de que en los años 2020 y el 2021 se estuvo brindando algún tipo de capacitación y eso que el nivel de ciberdelitos aumento debido a la pandemia del covid-19 pero la mayoría de personas estafas por las redes sociales su denuncia no progreso debido a que la policía no está capacidad para hacer el rastreo de los delitos por lo mismo los delincuente abusan de esta deficiencia que tiene el ministerio publico</p>	<p>solamente participe en la universidad en algunas capacitaciones pero en la policía no nos brindan esos mecanismos para poder combatir la ciberlincuencia si bien es cierto tenemos una división que es la DIVINDAT que significa que combate los delitos de alta tecnología pero la verdad no se da abasto si fuera posible el estado peruano debería invertir en capacitaciones de su personal policial para poder reducir la delincuencia como ahora tenemos los gota gota que es a</p>	<p>No nunca participe tampoco he visto casos de delitos informáticos pero la verdad es que no tengo el conocimiento para poder investigar más sobre el tema debido a que el ministerio publico carece mucho de conocimientos de nuevos delitos cibernéticos por lo mismo nosotros nos agenciamos de varios videos para poder ver cuáles son las nuevas tecnologías delictivas pero la policía no brinda hasta la actualidad , debería si</p>

ocasionando así que la mayoría de veces quede en la impunidad .

través de préstamos por aplicaciones que reduzca la delincuencia en Trujillo.

descargadas del play store y termina en un caso de extorción.

Interpretaciones las entrevistas realizadas a los especialistas, 1 y 2 establecen que no han podido participar de capacitaciones relacionadas con los delitos cibernéticos a consecuencia de que el estado no les brinda el apoyo necesario para capacitarse; y los especialistas 3,4,5,6, manifiestan que asistieron a capacitaciones de manera particular, es decir invirtieron su propio dinero para estar capacitados y poder actuar frente a loa delitos informáticos que asechan a la sociedad.

Fuente 7: Entrevistas aplicadas a especialistas

Tabla 10:

La logística que brinda las instituciones públicas para combatir los delitos informáticos en Trujillo.

PREGUNTA 09: ¿Qué logística le brindo su institución para combatir el incremento de los delitos informáticos en la ciudad de Trujillo en los años 2020-2021?

E1	E2	E3
En el ministerio público no me brindaron ninguna logística debido a que la área especializada para este tipo de delitos informáticos está en Lima por ende se	La policía no tiene logística solamente cumplimos nosotros el trabajo de arrestar si están en fragancia o recepcionar las denuncias de las personas que fueron en	La logística que me brindaron fueron solamente recolectar las manifestación y hacer una breve descripción de las denuncias de suplantación de identidad

<p>puede pedir alguna asesoría externa para poder resolver por el momento este tipo de delitos, ya que no tenemos capacitaciones herramientas como computadores ,software que puedan ayudarnos a combatir a los delincuentes a también como un buen internet que no sea lento y muchas herramientas más que necesita la fiscalía para poder llegar a formalizar sus denuncias.</p>	<p>esta caso defraudadas como son la suplantación de identidad o el robo sistemático de información o de cuentas bancarias, debido a que los únicos que investigan este tipo de delitos son la DIVINDAT o la fiscalía porque ellos tienen un mayor conocimiento debido a que mi institución policial no me brinda las alternativas necesarias para combatir la delincuencia.</p>	<p>para tener una cifra exacta de números de incidencias por esta clase de delitos y la mayoría de delitos van en aumento debido a eso la fiscalía está poniendo mayor empeño para poder combatir este tipo de delitos informáticos porque cada día tienen nuevas formas si bien es cierto no contamos con una fiscalía especializada pero no nos rendimos y estamos poniendo de nuestra parte para combatirla .</p>
--	--	--

E4

E5

E6

<p>No, ningún tipo de rol me brindo la policía debido a que mi comisaria solo recepción a las denuncias, pero no las investiga a fondo solamente tenemos que limitarnos a ciertas cosas y no podemos indagar más me gustaría pertenecer a otra área como la Divindat, pero ya sería más adelante que me pueda capacitar para poder desallorar mejor el tema y tener el</p>	<p>Sí, me brindaron alguno tips para combatir los delitos informáticos, pero fueron simples no fue una clase de capacitación fueron alguno tips breves del comisario donde se nos informó cómo están operando ahora los delincuentes por eso tenemos que usar nuevas alternativas para tener a los delincuentes atrás de las rejas.</p>	<p>claro realizamos muchos operativos con el fin de recepcionar los teléfonos donde operaban los ciberdelincuentes a través de perfiles falsos haciéndose a sí de cuantiosas sumas de dinero a través de las estafas por redes sociales por lo mismo nosotros realizamos operativos para corroborar los IMEI de los celulares si eran robados o estaban reportados</p>
--	---	--

conocimiento previo para ayudar a mi comisaria que mucha falta le hace tener nueva tecnología y herramientas necesarias.

como extraviados por lo mismo combatimos con ese método a los delincuentes para que no también recepción artículos robados.

INTERPRETACIÓN: De los 6 especialistas han constatado que la normativa vigente es insuficiente para hacer frente a la ciberdelincuencia y, en consecuencia, a la seguridad actual porque, a pesar de la existencia de una pena y de la aplicación de la misma, los delincuentes responsables que están libres siguen operando y manteniendo las formas delictivas, y en otros casos, como el fraude informático que genera ingresos, los delincuentes siguen en libertad por falta de medios para combatirlos. En base a lo expuesto, recomiendan la creación de una nueva fiscalía de delitos informáticos que se adecue a la realidad actual o, en todo caso, que la pena sea más severa y que además existan mayores facilidades para su formalización, como por ejemplo menos tiempo. Además, solicitan un acuerdo del gobierno para capacitar a la policía y a la fiscalía e implementar diversas herramientas tecnológicas en la ciudad de Trujillo.

Fuente 8: Entrevistas aplicadas a especialista.

RESULTADO DE OBJETIVO ESPECIFICO 03: Respecto al resultado se ha evidenciado que las herramientas digitales que tienen las instituciones públicas como la fiscalía y la policía nacional del Perú no son suficientes para dar solución a la ciberdelincuencia y por ende a la seguridad existente porque si bien es cierto existe una fiscalía especializada en delitos cibernéticos pero esta fiscalía se encuentra en la ciudad de Lima ,por eso es necesario la creación de una fiscalía especializada como medida alternativa de solución para combatir la ciberdelincuencia en la ciudad de Trujillo .Se puede apreciar que la mayoría de las personas entrevistadas no cuentan con una capacitación sobre delitos informáticos sabiendo que estas modalidades delictivas son nuevas en nuestro país por ende se debe capacitar a las instituciones públicas con el fin de combatir los delitos informáticos y así reducir la tazas de incremento que se vienen generando por la falta de conocimientos por parte de las autoridades competentes. Para que realicen su labor y no tengan ningún tipo de impedimento y poder realizar las investigaciones del caso para poder acusar al ciberdelincuente ya que es muy difícil poder encontrar a estos delincuentes sin una capacitación permanente y las herramientas digitales que deberían brindarles la institución a la cual representan. La logística brindada por parte de las entidades del estado es muy deficiente comparada al hacker que tienen una tecnología de punta comparado con las instituciones públicas no se puede competir al mismo ritmo debido a que ellos cuentan con herramientas digitales sofisticados.

4.2 DISCUSIÓN

Se tuvo en cuenta los datos cualitativos obtenidos y reflejados en las tablas para poder realizar correctamente el apartado de la Discusión. Así mismo, los precedentes internacionales y nacionales no han encontrado investigaciones previas a nivel local. Cabe señalar que los hallazgos también se compararon con diferentes enfoques teóricos y conceptuales. Así mismo respecto al **primer objetivo específico**; se identificó que tipos de modalidades de delincuencia cibernética se dieron con más frecuencia en Trujillo, es así que como en la entrevista aplicada a los 6 especialistas se obtuvo resultado que los delitos realizados con más frecuencia (ver tabla 1), son : robo de identidad, estafa piramidal, estafa de créditos bancarios, delito de hacker de información de cuentas bancarias y suplantación de identidad por redes sociales, de los cuales se produce por el mal manejo de la tecnología; también se logró apreciar que para combatir la delincuencia cibernética en la ciudad de Trujillo no se cuenta con los medios suficientes debido a la falta de presupuesto que el gobierno imparte en su presupuesto anual es por eso que la fiscalía y las dependencias policiales no cuentan con una capacitación o con herramientas digitales para poder combatir la delincuencia cibernética (ver tabla 2). Los roles que las entidades bancarias tienen que tomar en cuenta son capacitar a sus clientes con el fin que no seas estafados o suplanten su identidad debido a los miles de transacciones bancarias que realizan a diario es por ello que los bancos deben estar en constante contacto con el cliente para que no caigan en alguna de los miles de estafas por internet (ver tabla 03). No se logra identificar los autos de los delitos de ciberdelincuencia debió a que la policía (Divindat) que es la policía encargada de los delitos de alta tecnología no está capacitada para realizar este trabajo es por eso que con la herramienta inadecuadas y la sobre carga procesal la fiscalía y la policía no se dan abasto para poder seguir los pasos de los autores de los ciberdelitos (ver tabla 4). Resultados que al ser comparados con lo encontrado por el autor Huamán (2020), que en su Investigación, concluyó que en el año 2017 el Perú de alguna manera era más propenso al ransomware con un 25.1% de lo general de asuntos mostrados; entonces en el 2019, nuestra nación era el tercer país en Latinoamérica más afectado con respecto a los esquemas Spyware; de igual en el propio año se 43

mostraron 3012 acusaciones por estafa informática y 247 acusaciones con respecto a la falsificación de identificación en la Divindat; a ello se incorpora lo que es el insuficiente presupuesto consignado a referir con tecnología de alta gama para con el seguimiento de este tipo de delitos. Por otro lado, la ONU (2019), nos indica que los métodos que diseñaron los malhechores que provocaron la ampliación de la tasa y la complejidad de las infracciones cometidas en la naturaleza digital y a través de él. En cuanto **al segundo objetivo específico**, que estuvo dirigido precisar cuál ha sido el nivel de aumento de delincuencia cibernética a causa del covid-19; en donde se analizó documentación del año 2020 y 2021 (ver tabla 7), de los cuales se pudo apreciar que los delitos y/o modalidades con mayor índice son la estafa, suplantación de identidad estos con referencia del año 2020 el cual el número de denuncias de una manera global ascienden a 266. Por consiguiente, en el año 2021 los delitos y/o modalidades en ascendencia fueron, robo de identidad, clonación de tarjetas, estafa cibernética, training. En base a nuestra entrevista realizada apreciamos que de manera general estos delitos ascienden a un número de denuncias de 356 en el año indicado

Estos resultados, se relacionan con lo encontrado con el autor Cadena (2011), en su ensayo titulado “crecimiento del Ciberfraude en Colombia a lo largo de la pandemia por covid-19”, concluyó que en Colombia se llegó a registrar entre el 2019 y el 2020 aumentó un 114% cifras que fueron entregadas por centro cibernético policial, pues se explica que los delitos que presentaron el aumento fueron principalmente la vulneración de datos personales donde estos dieron paso a la violación de la información de los sitios web producido contundentes robos cibernéticos. Por otro lado, Acosta (2020), señala que como “actos ilícitos ocurridos mediante el gasto impropio de la tecnología, arremetiendo contra la intimidad de la averiguación de terceras personas, perjudicando o quitando algún tipo de datos que se descubren acumulados en servidores o gadgets”. El cual se refiere al aumento de la delincuencia cibernética en la ciudad de Trujillo, es así que el ministerio lidio con varios casos de delitos informáticos en el año 2021 a diferencia del año 2022 en el cual atendió una cifra mayor de casos de delitos informáticos pero sobre todo de suplantación de identidad y fraude informático que para el ministerio 44 público y la policía nacional del Perú son los delitos con mayor reincidencia ,la comisión de

estos delitos es cada día más común debido a que existe un vacío legal cuando se trata de hechos delictivos de carácter tecnológico y con una deficiencia de recursos para realizar investigaciones iniciales por parte de las autoridades correspondientes. Así mismo, Vílchez (2020), manifiesta que debido a la crisis sanitaria que han sufrido todos los países del mundo durante la pandemia del covid-19, se han desarrollado muchas relaciones sociales y económicas a través del uso de herramientas tecnológicas, para investigar y perseguir el ciberdelito, falta la formación policial y el uso de conocimientos técnicos. Por lo tanto, apoyando los objetivos en los trabajos analizados anteriormente, Zevallos (2020), explica que uno de los retos para que el Perú implemente una transformación digital es considerar los riesgos de vulnerabilidad de la seguridad informática; es necesario proteger la infraestructura de la información y crear un consejo de ciberseguridad con el objetivo de generar una gestión de riesgos informáticos; y, por ello, es necesaria la colaboración de la información tanto en el sector público como privado para denunciar los ciberataques y brindar a los usuarios información de seguridad informática.. Con lo que respecta al segundo objetivo específico se puede apreciar que tanto la policía nacional del Perú, como la fiscalía, necesitan ser capacitados con herramientas tecnológicas y poder tener cursos especializados en delitos informáticos, para poder llevar a cabo una correcta investigación de dichos delitos y condenar a quienes resulten responsables de estos.

El tercer objetivo específico, se evidencio por medio de las entrevistas que, necesariamente, se necesita de la creación de una fiscalía especializada en delitos informáticos en la ciudad de Trujillo con el fin de poder combatir la delincuencia cibernética, debido a que la fiscalía, actualmente, no cuentan con herramientas digitales para poder saber quiénes son los autores de los delitos cibernéticos, como la suplantación de identidad o el fraude informático; delitos que necesariamente necesitan una serie capacitaciones adecuada al tema para poder desarrollar mejor las funciones de investigación y así poder estar a la vanguardia con las nuevas modalidades delictivas ya que por ahora no se tiene una logística adecuada para poder prevenir de este tipo de delitos a la población debido a la falta de conocimiento por parte de los representantes del ministerio público como también de la policía nacional del Perú, (ver tabla 8, 9 y 10).

Lo descrito previamente, está relacionado con lo citado por Chocobar (2019), quien llegó a la conclusión que el Perú debe realizar gastos en seguridad digital y así crear una cultura de ciberseguridad y defensa digital, para evitar que muchas personas sean objeto de posibles ciberataques.

Salazar (2019), describe cómo las innovadoras herramientas tecnológicas se han visto afectadas por la evolución de los ciberdelitos y que no asegura el entorno virtual. Dado que cualquier transacción financiera o pago electrónico la persona puede ser víctima de un fraude cibernético, el comercio en línea plantea problemas de seguridad. A su vez, los doctores Rodríguez et al. (2020), Considera que los delitos informáticos deben ser sancionados porque actualmente son el medio más utilizado por los delincuentes para cometer fraudes cibernéticos. Sin embargo, considera que debido a que el reglamento de la Ley 30096 no está basado en nuestra realidad social, algunos de sus artículos carecen de lógica y producen confusión al momento de aplicar la ley. En este contexto, hace referencia a que muchas de las naciones que han ratificado el Convenio de Budapest han cambiado sus leyes para reflejar mejor las realidades sociales de cada nación, ya que la existencia de pistas no se puede ser asumida al momento de imputar el delito. Sin embargo, dado que el lenguaje de la Ley N° 30096 es tan similar al del Convenio de Budapest y dado que existe un escaso conocimiento sobre los alcances de los delitos informáticos, el Perú aún no se ha adelantado a este evidente vacío. En consecuencia, es necesario que haya suficiente publicidad para la prevención del delito porque son comportamientos que tienen el potencial de infligir daño. Si bien es cierto que se trata de un problema complejo en cuanto a su tratamiento, hay que idear soluciones para evitar la impunidad del delito porque los métodos utilizados para su realización están cambiando también porque la tecnología evoluciona y no es estática, a diferencia de los delitos anteriores.

V.CONCLUSIONES

PRIMERO: En la ciudad de Trujillo, las causales del incremento de los ciberdelitos fue la pandemia del covid19, que dejó a muchas personas sin empleo, es decir, la mayoría de personas tuvo que dejar sus trabajos para poder estar en un aislamiento obligatorio debido a la crisis sanitaria, es así que aumentó la delincuencia cibernética. También se puede hacer mención al hecho que la moneda digital, como el yape y el plim, se utilizaron en pandemia para poder realizar transacciones sin poder tener algún tipo de contacto por el miedo de ser contagiado con el covid-19, lo cual lo convirtió en un factor importante del incremento de los ciberdelitos, pues aumentaron las estafas como suplantación de identidad y fraude informático.

SEGUNDO: En la ciudad de Trujillo los delitos con mayor frecuencia son: los delitos de fraude informático y suplantación de identidad aumentaron significativamente entre 2020 y 2021. Lo cual se incrementó debido a que las personas realizan sus compras a través de plataformas digitales y ahora con la moneda digital tales como el yape y el plim, Esto aumentó las estafas cibernéticas debido a que las personas ingresan sus datos como claves bancarias, es por eso que la mayoría de delitos son también de suplantación de identidad porque la mayoría de personas ingresan sus datos a redes sociales como el Facebook o Instagram y diferentes plataformas digitales y los ciberdelincuentes toman esos datos para suplantar la identidad de las personas, el insaciable deseo de conexión de la generación actual ha alimentado el crecimiento exponencial de las tecnologías de la información y la comunicación, lo que ha acelerado el ritmo de comisión de delitos informáticos. Para salvaguardar la integridad y la privacidad de las personas, hay que tener en cuenta la necesidad de prohibir y castigar el uso no autorizado de información personal de las redes sociales. Los delitos informáticos suelen repercutir no sólo en la intimidad de las personas, sino también en la sociedad en su conjunto.

TERCERO: De los resultados obtenidos en el análisis documentario se logró apreciar el nivel de aumento de la ciberdelincuencia en la ciudad de Trujillo con un porcentaje del 78% de aumento entre los años 2020 al 2021. Los delitos informáticos son una nueva modalidad de robo que se ha popularizado en los últimos años sobre todo en pandemia, esto ha aumentado ya que muchas personas se ven obligadas a comprar en línea como también a realizar operaciones bancarias u otros servicios en línea como los pagos de recibos de servicios. Este tipo de delitos se han convertido en una ventana del crimen, donde los delincuentes encuentran la excusa perfecta para robar el dinero de otras personas en transacciones en línea, el ministerio publico recobra a diario nuevos datos de ciberdelincuencia es así que cada día aumenta los delitos informáticos en nuestra ciudad Trujillo .En nuestro análisis documentario se puede apreciar que en estos últimos años los delitos informáticos aumentaron de tal manera que el ministerio público recibió varias denuncias en el año 2021, también se logra apreciar que en el año 2022 los delitos informáticos fueron mayores a nivel de Trujillo cifras brindadas por el ministerio público. Por ello logramos apreciar un incremento entre los años 2021 al 2022 debido a la creación de la moneda digitales como el yape y el plim ya que este tipo de monedas digitales se utilizan para realizar transacciones diarias sin tener una moneda física es por eso que las estafas cibernéticas aumentaron.

CUARTO: Entre las alternativas de solución que se pueden proporcionar, para frenar la comisión de los delitos de ciberdelincuencia en Trujillo 2020-2021, serían las siguientes: Que la PNP y MP cuentan con las herramientas necesarias para desarrollar mecanismos que sirvan para combatir la ciberdelincuencia, es por ello que el estado peruano debería realizar inversión para poder capacitar y tener herramientas digitales para poder salvaguardar el patrimonio de los ciudadanos que muchas veces son víctimas de estafas cibernéticas por realizar compras por internet. Asimismo, las entidades públicas deberían contar con la infraestructura necesaria para poder realizar las diligencias pertinentes para el autor de los delitos informáticos, es por eso que se debe llevar a cabo capacitaciones para poder tener un personal que cumpla con su desenvolvimiento de manera exitosa, dándole todas las herramientas posible para poder cumplir su función al 100% y también

desarrollar medidas de protección contra los ciberataques que los ciberdelincuentes logran hacer contra empresas y también contra personas que manejan cuentas digitales , Sin embargo, las redes sociales también pueden utilizarse para cometer delitos, lo que dificulta la identificación de los responsables al no existir herramientas digitales que protejan nuestra identidad. Las redes sociales pueden utilizarse para conectar a personas que pueden o no tener intereses similares o para proporcionar plataformas de comunicación e información.

VI. RECOMENDACIONES

Una vez realizado el análisis del estudio y las entrevistas a las comisarías de la ciudad de Trujillo y a los representantes del Ministerio Público se presenta las respectivas recomendaciones a fin de que pueden ayudar a mejorar las dificultades que presente los órganos jurisdiccionales.

PRIMERO: La División de Investigación de Delitos de Alta Tecnología (DIVINDAT) ponga mayor énfasis al cumplir su misión para combatir delitos de esta índole, a través de un profundo seguimiento a dispositivos utilizados por los ciberdelincuentes para poder rastrearlos, ubicarlos y ponerlos a disposición de la justicia, crear sitios seguros para las personas en donde se almacenen datos personales y económicos difícilmente de ser hackeados para beneficio del delincuente, para así evitar el incremento de la ciberdelincuencia.

SEGUNDO: Se les insta a las personas a que deben encontrarse bien informados sobre los delitos cibernéticos que amenazan las redes hoy en día, al realizar un compra a través de una página en internet se tiene que hacer en modo privado ya que al momento de cerrar dicha página esta se borra toda información y así de esa manera los cracker cibernéticos no podrán acceder a tus datos personales de igual forma se recomienda no ingresar a links que promocionan en la redes o a través de los mensajes de texto especialmente cuando estos requieran de sus tarjetas.

TERCERO: El Ministerio Público especializada en delitos informáticos debe tomar precauciones y un manejo audaz y rápido en cuanto a los sucesos ocurridos, con el fin de dar con los responsables, sin que éstos pasen desapercibidos. puesto que en los últimos años y a raíz del covid-19 se notó un aumento considerable, en cuanto no menos importante cabe señalar que sería favorable cierta capacitación a las personas sobre el uso, manejo, y consecuencias de estos medios tecnológicos, para no caer en las fechorías de estos especialistas en robos cibernéticos y sobre todo la creación de una fiscalía especializada en ciberdelincuencia en la ciudad de Trujillo con el fin de poder combatir los ciberdelitos en Trujillo.

REFERENCIAS

Acosta, M., Benavides, M. y García, N. (2020). Delitos informáticos: Impunidad organizacional y su complejidad en el mundo de los negocios. *Revista Venezolana de Gerencia*, 25(89), 351–368.
<https://doi.org/10.37960/revista.v25i89.31534>

Agudo, E., Jaén, M., y Perrino, Á. L. (2019). *Derecho penal aplicado. Parte especial. Delitos contra el patrimonio y contra el orden socioeconómico*. (1° Ed.). Dykinson.

Beiersmann, S. (2018). *WhatsApp: Alcances de una nueva aplicación*. (2° Ed.). Ediciones Comillas.

American Thoracic Society SALUD DEL PACIENTE | SERIES INFORMATIVAS
www.thoracic.org CLIP AND COPY. (n.d.).

<https://www.thoracic.org/patients/patient-resources/resources/spanish/covid-19.pdf>

Abreu, J. L. (2014). El Método de la Investigación. *Daena: International Journal of Good Conscience*, 6.

[http://www.spentamexico.org/v9-n3/A17.9\(3\)195-204.pdf](http://www.spentamexico.org/v9-n3/A17.9(3)195-204.pdf)

Acosta, M (2020). *Delitos informáticos: impunidad organizacional y su complejidad en el mundo de los negocios*. Revista Venezolana de Gerencia. EDITORIAL. Universidad del Zulia. Venezuela.

<https://www.redalyc.org/journal/290/29062641023/29062641023.pdf>

Agamben, G. (2016). Que es un dispositivo. 22.

<https://www.redalyc.org/journal/290/29062641023/29062641023.pdf>

Arteaga, G. (2020). ¿Qué es el análisis de datos? Método, técnicas y herramientas. *Recogida y Análisis de datos*, 2.

<https://www.testsiteforme.com/tecnica-de-procesamiento-y-analisis-de-datos/>

Benadiba y Plotinsky (2020). La entrevista en la investigación cualitativa.

[https://investigaliacr.com/investigacion/la-entrevista-en-la-investigacion-cualitativa/#:~:text=La%20entrevista%20es%20una%20conversaci%C3%B3n,48\).](https://investigaliacr.com/investigacion/la-entrevista-en-la-investigacion-cualitativa/#:~:text=La%20entrevista%20es%20una%20conversaci%C3%B3n,48).)

Choucri, (2017). *El sistema internacional cibernético*. Asuntos internacionales. Recuperado INTERPOL, (agosto,2020). Ciberdelincuencia: Efectos de la COVID 19. Lyon – Francia: Secretaría General de INTERPOL.

file:///C:/Users/usuario/Downloads/COVID-19%20Cybercrime%20Analysis%20Report-Design_02_SP.pdf

Colmex (2018). Enfoques, definiciones y estimaciones de pobreza y desigualdad en América Latina y el Caribe.

https://repositorio.cepal.org/bitstream/handle/11362/46405/4/S2100026_es.pdf

Crecimiento Del Ciberfraude En Colombia Durante La Pandemia Por Covid-19 [ARCHIVO PDF]

[Cadena Alvarado Ana María 2021.pdf \(unimilitar.edu.co\)](#)

Glaser, B. G., & Strauss, A. (1967). *The Discovery of Grounded Theory*. Hawthorne, New York: Aldine de Gruyter.

http://www.sxf.uevora.pt/wp-content/uploads/2013/03/Glaser_1967.pdf

González, C. (2020, 24 de abril). Cómo está afectando la expansión del COVID-19 a la ciberdelincuencia. BBVA NOTICIAS; BBVA.

<https://www.bbva.com/es/como-esta-afectando-la-expansion-del-covid-19-a-la-ciberdelincuencia/>

Gonzalo Varillas (2020). Divincri reporta 20 robos cibernéticos en Piura.

<https://walac.pe/divincri-reporta-20-robos-ciberneticos-en-la-region-piura/>

Gracia, Y (2018). uso correcto e incorrecto de la tecnología. (Prezi.com.

<https://prezi.com/ni2ttetrvqie/uso-correcto-e-incorrecto-de-la-tecnologia/>

Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, P. (2014). *Metodología de la Investigación*. México: McGRAW-HILL/ INTERAMERICANA EDITORES, S.A. DE C.V.

https://www.academia.edu/36750638/METODOLOGIA_DE_LA_INVESTIGACION_Hern%C3%A1ndez_Fernandez_y_Babtista_5ta_Edicion

Horianski, J.E (2018). Trabajo final de graduación la protección penal ante el avance tecnológico y la delincuencia cibernética"Dado el carácter transnacional ¿es suficiente la normativa penal existente para impedir el avance de la ciberdelincuencia.

<https://repositorio.uesiglo21.edu.ar/bitstream/handle/ues21/14687/HORIANSKI%20JORGE.pdf?sequence=1>

HUAMAN CRUZ, M. Y. (2020). LOS DELITOS INFORMÁTICOS EN PERÚ Y LA SUSCRIPCIÓN DEL. *Tesis para optar al título profesional de Abogada*. UNIVERSIDAD ANDINA DE CUSCO, Cusco - Perú.

https://repositorio.uandina.edu.pe/bitstream/handle/20.500.12557/4116/Marleny_Tesis_bachiller_2020.pdf?sequence=1&isAllowed=y

HUAYRE TORRES, I. G. (2021).El impacto del cibercrimen en delitos de estafa en el Distrito de Lima, 2021. *PARA OPTAR EL TÍTULO PROFESIONAL EN DERECHO*. UNIVERSIDAD PERUANA DE LAS AMÉRICAS, Lima - Perú.

<http://repositorio.ulasamericas.edu.pe/bitstream/handle/upa/1729/TRABAJO%20DE%20INVESTIGACION%20N%20%281%29.pdf?sequence=1&isAllowed=y>

Kemmis y Mc Taggart (2020). Investigación básica: características, definición, ejemplos. Lidefer. Recuperado de <https://www.lifeder.com/investigacion-basica/>

Laudon y Guercio (2018), Factores que influyen en la compra online y el comportamiento de los consumidores del distrito de San Miguel en el año 2020 (tesis de Bachiller, Universidad Nacional Mayor de San Marcos).

<https://cybertesis.unmsm.edu.pe/bitstream/handle/20.500.12672/16425/Guarnizogg.pdf?sequence=1&isAllowed=y>

Litchfiel (2017). DESIGUALDAD.

https://scholar.harvard.edu/files/vrios/files/201508_mexicoinequality.pdf?m=1453513192

López, E. A. (23 de enero de 2022). metodología cualitativa. Obtenido de

https://www.eumed.net/tesis-doctorales/2012/eal/metodologia_cualitativa.html

Ministerio Público. (febrero 2021). Informe de Análisis N°4 - Ciberdelincuencia: Pautas para una Investigación Fiscal Especializada. Lima - Perú: Fiscalía de la Nación.

Moisés J. Schwartz (2020), Ciberseguridad, riesgos, avances y el camino a seguir en América latina y el caribe.

<https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf>

OCHOA, D. A. (2013), La Teoría Fundamentada como metodología para la integración del análisis procesual y estructural en la investigación de las Representaciones Sociales. *Revista CES Psicología ISSN 2011-3080*, 6(1), 126,127. redalyc.org/pdf/4235/423539419008.pdf

Oficina de las Naciones Unidas, (2019). *ciberdelincuencia en el Perú: pautas para una investigación fiscal especializada*, Editorial, OFAEC.

OIT (2017), Perú: Participación de la Población en la Actividad Económica, 2017.

https://www.inei.gob.pe/media/MenuRecursivo/publicaciones_digitales/Est/Lib1676/06.pdf

Organización de las Naciones Unidas Para la Educación, la Ciencia y la Cultura. (1 de Julio de 2017). *Información Falsa: la Opinión de Periodistas*.

[https://es.unesco.org/courier/july-september-2017/informacion-falsa-opinion-periodistas.](https://es.unesco.org/courier/july-september-2017/informacion-falsa-opinion-periodistas)

Organización Internacional De Política Criminal (2020), informe de interpol muestra un aumento alarmante de los ciberataques. Durante la epidemia de COVID-19.

[https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2020/Un-informe-de-INTERPOL-muestra-un-aumento-alarmante-de-los-ciberataques-durante-la-epidemia-de-COVID-19?msclkid=a7cb28c7c7dc11ec97df51b6c39ee611.](https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2020/Un-informe-de-INTERPOL-muestra-un-aumento-alarmante-de-los-ciberataques-durante-la-epidemia-de-COVID-19?msclkid=a7cb28c7c7dc11ec97df51b6c39ee611)

(Pardo Vargas, 2018), en su tesis “Tratamiento jurídico penal de los delitos informáticos contra el patrimonio, Distrito Judicial de Trujillo, 2018”

[http://repositorio.unu.edu.pe/bitstream/handle/UNU/5184/B02_2022_UNU_CONTABILIDAD_T_2021_ALEXIS-MARIN_ESTEFANY-SANTAMARIA.pdf.](http://repositorio.unu.edu.pe/bitstream/handle/UNU/5184/B02_2022_UNU_CONTABILIDAD_T_2021_ALEXIS-MARIN_ESTEFANY-SANTAMARIA.pdf)

Ratcliffe y Gonzales del Valle (2011). La entrevista. Obtenido de

Rojas Crotte, I. R (2016). Tiempo de Educar: Elementos Para el Diseño de Técnicas de Investigación: Una Propuesta de Definiciones y Procedimientos en la Investigación Científica 12 (24) P.278.

Rubén Permuy Iglesias. (2020), La crisis del coronavirus aumenta la ciberdelincuencia. UOC (Universitat Oberta de Catalunya); UOC.

[https://www.uoc.edu/portal/es/news/actualitat/2020/178-coronavirus-aumento-ciberdelincuencia.html.](https://www.uoc.edu/portal/es/news/actualitat/2020/178-coronavirus-aumento-ciberdelincuencia.html)

Torres, R. R. (24 de julio de 2019). manual de investigación. Obtenido de

[https://tesisplus.com/metodo-inductivo/metodo-inductivo-segun-autores/#:~:text=El%20autor%20Rodolfo%20Rivas%20Torres%2C%20en%20su%20libro,y%20costumbres%20Litchfield%20observadas%20a%20partir%20de%20casos%20particulares.](https://tesisplus.com/metodo-inductivo/metodo-inductivo-segun-autores/#:~:text=El%20autor%20Rodolfo%20Rivas%20Torres%2C%20en%20su%20libro,y%20costumbres%20Litchfield%20observadas%20a%20partir%20de%20casos%20particulares)

Valentín Cimino (2022, March 24), Le FBI estime que la cybercriminalité a coûté 6,3 milliards d'euros au cours de l'année passée. Siècle Digital.

<https://siecledigital.fr/2022/03/24/le-fbi-estime-que-la-cybercriminalite-a-coute-63-milliards-deuros-en-2021/>

Vargas, J. (2018, 19 de enero). "Crackers", los verdaderos ciberdelincuentes. Tiempo; Hora.

<https://www.eltiempo.com/tecnosfera/novedades-tecnologia/crackers-los-verdaderos-delincuentes-ciberneticos-173052>.

Villavicencio (2014). Ciberdelincuencia en el Perú: pautas para una investigación fiscal especializada. [ARCHIVO PDF].

<https://cdn.www.gob.pe/uploads/document/file/1669400/CIBERDELINCUENCIA%20EN%20EL%20PERU%CC%81%20-%20PAUTAS%20PARA%20SU%20INVESTIGACION%CC%81N%20FISCAL%20E%20SPECIALIZADA%20-%202015%20FEBRERO%202021.pdf>

Diagnostico situacional sobre la Ciberdelincuencia en el Perú estadística DIVINDAT- DIRINCRI PNP. (2020).

Recuperado <https://cdn.www.gob.pe/com>

Espinoza Coila, M. (2017), *Derecho penal informático: deslegitimación del poder punitivo en la sociedad de control*. Recuperado de <http://repositorio.unap.edu.pe/handle/UNAP/6309>.

Flores M. (2018), Tecnología y violencia en Perú. En Hiper derecho. Recuperado de <https://bit.ly/3oJbmbf>.

Fuentes Garrido K. (2021), Modificación de la ley 30096 para incorporar los delitos de phishing, pharming y carding como delitos penalizables con prisión, para reducir la ciberdelincuencia, lima 2019. Recuperado de <https://repositorio.uss.edu.pe/handle/20.500.12802/8345>.

Informe N°4 del Ministerio Publico y la oficina de análisis de estratégico contra la criminalidad. (2021), Recuperado de <file:///C:/Users/usuario/Documents/%20QUE%20USO/Informe%20N%C2%B04%20Unidad%20Fiscal%20Ciberdelincuencia.pdf>.

Informe de la policía nacional del Perú dirección de investigación criminal división de investigación de delitos de alta tecnología N°113. (2020).

LP Pasión por el Derecho (2020). Delitos de peligro abstracto y concreto. Recuperado de <https://lpderecho.pe/tag/delitos-de-peligro-abstracto/>

LP Pasión por el Derecho (2020). Tipos penales. Recuperado de <https://lpderecho.pe/cuales-son-las-clases-de-tipos-penales-bien-explicado/>.

ANEXOS

ANEXOS

Anexo 01. Matriz de categorización

Título: Incremento de los delitos informáticos a consecuencia de la pandemia del Covid-19 en la ciudad de Trujillo entre los años 2020-2021				
Problemas	Objetivos	Supuestos	Categorías /subcategorías	Metodología
<p>Problema general ¿Cuáles fueron las causas que influyeron en el incremento de la delincuencia cibernética a consecuencia del covid-19 en Trujillo 2020-2021?</p>	<p>Objetivo general Determinar las causales del incremento de delincuencia cibernética en tiempos de aislamiento social obligatorio producto del covid19.</p>	<p>Supuesto general Los principales delitos que se cometieron en la ciudad de Trujillo en los años 2020-2021 fueron los delitos de suplantación de identidad y de fraude informático.</p>	<p>Categoría 1 Delitos informáticos</p> <p>Subcategorías Criminalidad informática Dispositivos de seguridad Uso inadecuado de la tecnología</p>	<p>Enfoque Cualitativo</p> <p>Diseño Teoría fundamentada</p>
<p>Problema específico 01 ¿Qué tipo de modalidades de delincuencia cibernética se dieron con más frecuencia en Trujillo 2021?</p> <p>Problema específico 02 ¿precisar cuál ha sido el nivel de aumento de delincuencia cibernética a causa del covid-19 Trujillo 20-2021?</p> <p>Problema específico 03 ¿Se desarrollaron alternativas para combatir la ciberdelincuencia en Trujillo 2020-2021?</p>	<p>Objetivo específico 01 Identificar qué tipo de modalidades de delincuencia cibernética se dieron con más frecuencia en Trujillo 2020-2021.</p> <p>Objetivo específico 02 Examinar cual ha sido el nivel de aumento de delincuencia cibernética a causa del covid-19 en Trujillo 2020-2021.</p> <p>Objetivo específico 03 Desarrollar las alternativas de solución para los delitos de ciberdelincuencia en Trujillo 2020-2021.</p>	<p>Supuesto específico 01 El aislamiento social conduciría un alto incremento de la delincuencia cibernética o quizás los pobladores de Trujillo no manejan de forma correcta los medios cibernéticos.</p> <p>Supuesto específico 02 Las autoridades desconocen de la delincuencia cibernética por la falta de capacitación en sus entidades donde vienen investigando este tipo de delitos informáticos</p>	<p>Categoría 2 Covid-19</p> <p>Subcategorías Hackers cibernéticos Tiendas online Información falsa</p>	<p>Escenario de estudio Trujillo</p> <p>Participantes Especialistas (fiscales y policías) en derecho penal informático</p> <p>Instrumentos Guía de entrevista Guía de análisis documental</p>

Anexo N° 02. Cuestionario de entrevista.

TÍTULO: “Incremento de los delitos informáticos a consecuencia de la pandemia del Covid-19 Trujillo 2020-2021”.

Datos generales del entrevistado (a)	
Nombre y apellidos:	
Institución en la que labora:	
Cargo:	
Especialidad:	
Reunión	
Link:	
Fecha y hora:	

INSTRUCCIONES. Leer minuciosamente cada interrogante y responder desde su experiencia laboral y los conocimientos adquiridos, con claridad y autenticidad, en vista de que, la información obtenida corresponde a los resultados del presente trabajo de investigación, cumpliendo –de esa manera– los objetivos del mismo.

OBJETIVO ESPECÍFICO 1: Identificar qué tipo de modalidades de delincuencia cibernética se dieron con más frecuencia en Trujillo 2020-2021.	
PREGUNTAS:	RESPUESTAS:
1. ¿Cuáles son los delitos en materia de ciberdelincuencia que tuvieron más incidencia en la ciudad de Trujillo entre el año 2020-2021?	
2. ¿Qué acciones se realizaron para combatir la ciberdelincuencia en la ciudad de Trujillo en los años 2020-2021?	
3. ¿Qué acciones se realizaron para	

<p>combatir la ciberdelincuencia en la ciudad de Trujillo en los años 2020-2021?</p> <p>4.¿Cuál fue el rol de las entidades bancarias/financieras para la búsqueda de soluciones en los delitos de ciberdelincuencia?</p>	
<p>5.¿En la actualidad, cuantos casos de delitos informáticos se encuentran en una etapa de juzgamiento en la ciudad de Trujillo en los años 2020-2021?</p> <p>6.¿Qué mecanismos o procedimientos faltan para una adecuada investigación en los delitos de ciberdelincuencia?</p>	
<p>OBJETIVO ESPECÍFICO 2: Examinar cuál ha sido el nivel de aumento de delincuencia cibernética a causa del COVID-19 en Trujillo 2020-2021.</p>	
<p>PREGUNTAS:</p>	<p>RESPUESTAS:</p>
<p>7.Nivel de aumento de los delitos cibernéticos entre los años 2020-2021.</p>	
<p>OBJETIVO ESPECÍFICO 3: Proponer lineamientos para lograr una adecuada asignación de recursos basados en el presupuesto participativo.</p>	
<p>PREGUNTAS:</p>	<p>RESPUESTAS:</p>

8. Desarrollar las alternativas de solución para los delitos de ciberdelincuencias en Trujillo 2020-2021.	
9. ¿En qué capacitaciones a participado en relación a los delitos informáticos en el año 2020-2021 en la ciudad de Trujillo?	
10. ¿Qué logística le brindo su institución para combatir el incremento de los delitos informáticos en la ciudad de Trujillo en los años 2020-2021?	

FUENTE: Elaboración propia del autor.



Anexo N° 3. Validación del instrumento por experto N° 1.

ANEXO

**Validación de instrumento
CARTA DE INVITACIÓN N° 01**

Trujillo 06, junio de 2023

Dra. Milagros Acuña Villanueva

Asunto: **Participación en juicio de expertos para validar instrumento de investigación cualitativa**

Me es grato dirigirme a Ud., para expresarle mi respeto y cordial saludo; respecto al asunto hacerle conocer que estoy realizando el trabajo de investigación de enfoque cualitativo titulado: **“Incremento de los delitos informáticos a consecuencia de la pandemia del Covid-19 en la ciudad de Trujillo entre los años 2020-2021 “**

Con el fin de obtener el título de abogado.

La presente investigación tiene por finalidad de determinar si la pandemia del SARSCoV-2 influyó en el incremento de la delincuencia cibernética en la ciudad de Trujillo; en consecuencia, se deben realizar entrevistas cuyas preguntas conformen el instrumento de evaluación de la presente investigación, que deben ser validadas por expertos, como lo es en el caso de su persona. En ese sentido, **la invitamos a colaborar con la investigación, validando en calidad de experto dicho instrumento de recolección de información.**

Seguros de su participación en calidad de experto para la validación del instrumento de recolección mencionado, se le alcanza el cuestionario de entrevista para su evaluación, adjuntando el formato que servirá para esbozar sus apreciaciones en relación a cada ítem del presente instrumento de investigación. Conocedores de su alto espíritu altruista, agradecemos por adelantado su colaboración.

Atentamente.

Flores Mori Cesar Eugenio

DNI N°47910045

Evaluación por juicio de expertos

Respetado juez: Usted ha sido seleccionado para evaluar el instrumento "Recolección de datos de la información". La evaluación del instrumento es de gran relevancia para lograr que sea válido y que los resultados obtenidos a partir de este sean utilizados eficientemente; aportando al quehacer psicológico. Agradecemos su valiosa colaboración.

1. Datos generales del juez

Nombre del juez:	
Grado profesional:	Maestría () Doctor ()
Área de formación académica:	Social () Clínica () Educativa () Organizacional ()
Áreas de experiencia profesional:	
Institución donde labora:	
Tiempo de experiencia profesional en el área:	2 a 4 años () Más de 5 años ()
Experiencia en Investigación Psicométrica: (si corresponde)	Trabajo(s) psicométricos realizados Título del estudio realizado.



2. Propósito de la evaluación:

Validar el contenido del instrumento, por juicio de expertos.

3. Datos de la escala:

Nombre de la Prueba:	Entrevista
Autores:	Flores Mori Cesar Eugenio
Procedencia:	Propia
Administración:	
Tiempo de aplicación:	
Ámbito de aplicación:	Ciudad de Trujillo
Significación:	Explicar Cómo está compuesta la escala (dimensiones, áreas, ítems por área, explicación breve de cuál es el objetivo de medición)

4. Soporte teórico:

La pandemia del coronavirus en el año 2020 y el dinero digital	- ¿Causó el incremento en el uso de la moneda digital?	En el mercado bancario y financiero, es importante que toda operación esté dotada de eficacia y dinamismo. A raíz de la declaratoria de emergencia sanitaria producto del virus SARSCoV-2 (Covid-19), los seres humanos evitamos la manipulación de monedas y billetes, con el propósito de contrarrestar los
Categorías	Subcategorías	Definición
Ley N° 30096 – Ley de delitos informáticos	- Acceso ilícito a datos y sistemas informáticos - Fraude informático - Suplantación de identidad	Los delitos informáticos implican la utilización de las tecnologías de la información para atentar contra el patrimonio, la fé pública y el mercado financiero. La legislación penal debe adaptarse al desarrollo de la tecnología, lo cual permitirá combatir la ciberdelincuencia. Perú es considerado un país con alta vulnerabilidad ante ataques cibernéticos.
	- ¿O en realidad las plataformas digitales bancarias adolecen de medidas de ciberseguridad?	contagios masivos. Ante ello, las entidades monetarias impulsaron el uso de plataformas digitales de pago (Yape, Plin, Tunki, etcétera), lo cual revolucionó el mercado y su uso se volvió obligatorio para realizar negocios con mayor facilidad (o como dicen los comerciales en la televisión: “Haz negocios desde el mueble de tu casa”).

5. Presentación de instrucciones para el juez:

A continuación, a usted le presento el instrumento de recolección de datos elaborado por: Flores Mori Cesar Eugenio en el año 2023. De acuerdo con los siguientes indicadores califique cada uno de los ítems según corresponda.

Categoría	Calificación	Indicador
CLARIDAD El ítem se comprende fácilmente, es decir, su sintáctica y semántica son adecuadas.	1. No cumple con el criterio	El ítem no es claro.
	2. Bajo Nivel	El ítem requiere bastantes modificaciones o una modificación muy grande en el uso de las palabras de acuerdo con su significado o por la ordenación de estas.
	3. Moderado nivel	Se requiere una modificación muy específica de algunos de los términos del ítem.

	4. Alto nivel	El ítem es claro, tiene semántica y sintaxis adecuada.
COHERENCIA El ítem tiene relación lógica con la dimensión o indicador que está midiendo.	1. totalmente en desacuerdo (no cumple con el criterio)	El ítem no tiene relación lógica con la dimensión.
	2. Desacuerdo (bajo nivel de acuerdo)	El ítem tiene una relación tangencial /lejana con la dimensión.
	3. Acuerdo (moderado nivel)	El ítem tiene una relación moderada con la dimensión que se está midiendo.
	4. Totalmente de Acuerdo (alto nivel)	El ítem se encuentra está relacionado con la dimensión que está midiendo.
RELEVANCIA El ítem es esencial o importante, es decir debe ser incluido.	1. No cumple con el criterio	El ítem puede ser eliminado sin que se vea afectada la medición de la dimensión.
	2. Bajo Nivel	El ítem tiene alguna relevancia, pero otro ítem puede estar incluyendo lo que mide éste.
	3. Moderado nivel	El ítem es relativamente importante.
	4. Alto nivel	El ítem es muy relevante y debe ser incluido.

Leer con detenimiento los ítems y calificar en una escala de 1 a 4 su valoración, así como solicitamos brinde sus observaciones que considere pertinente

1 no cumple con el criterio
2. Bajo Nivel
3. Moderado nivel
4. Alto nivel

Dimensiones del instrumento:

- Primera dimensión:
Título: Incremento de los delitos informáticos a consecuencia de la pandemia del Covid-19 en la ciudad de Trujillo entre los años 2020-2021
- Objetivos específico: Identificar qué tipo de modalidades de delincuencia cibernética se dieron con más frecuencia en Trujillo 2020-2021. □ Categoría: Incremento de los delitos informáticos.

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones

Situaciones adversas	¿Cuáles son los delitos en materia de ciberdelincuencia que tuvieron más incidencia en la ciudad de Trujillo entre el año 2020-2021?	4	4	4	
Objetivo	¿Qué acciones se realizaron para combatir la ciberdelincuencia en la ciudad de Trujillo en los años 2020-2021? ¿Cuál fue el rol de las entidades bancarias/financieras para la búsqueda de soluciones en los delitos de ciberdelincuencia?	4	4	4	
Procedimiento	¿Qué tan difícil han sido identificar a los autores de los delitos de ciberdelincuencia en la ciudad de Trujillo 2020-2021? ¿En la actualidad, cuantos casos de delitos informáticos se encuentran en una etapa de juzgamiento en la ciudad de Trujillo en los años 2020-2021? ¿Qué mecanismos o procedimientos faltan para una adecuada investigación en los delitos de ciberdelincuencia?	4	4	4	

- Segunda dimensión: Desarrollar las soluciones, alternativas y su incidencia en la actividad cibercriminal □
Objetivos 3 de la Dimensión: Desarrollar las alternativas de solución para los delitos de ciberdelincuencias en Trujillo 2020-2021.

Pd.: el presente formato debe tomar en cuenta:

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
Modalidades de ciberdelincuencia	¿Resultaría necesario la creación de una fiscalía especializada en ciberdelincuencia en la ciudad de Trujillo? ¿por qué?	4	4	4	
Causas de la Ciberdelincuencia	¿En qué capacitaciones a participado en relación a los delitos informáticos en el año 2020-2021 en la ciudad de Trujillo?	4	4	4	
Incremento de la Ciberdelincuencia	¿Qué logística le brindo su institución para combatir el incremento de los delitos informáticos en la ciudad de Trujillo en los años 2020-2021?	4	4	4	

Williams y Webb (1994) así como Powell (2003), mencionan que no existe un consenso respecto al número de expertos a emplear. Por otra parte, el número de jueces que se debe emplear en un juicio depende del nivel de experticia y de la diversidad del conocimiento. Así, mientras Gable y Wolf (1993), Grant y Davis (1997), y Lynn (1986) (citados en McGartland et al. 2003) sugieren un rango de **2 hasta 20 expertos**, Hyrkäs et al. (2003) manifiestan que **10 expertos** brindarán una estimación confiable de la validez de contenido de un instrumento (cantidad mínimamente recomendable para construcciones de nuevos instrumentos). Si un 80 % de los expertos han estado de acuerdo con la validez de un ítem éste puede ser incorporado al instrumento (Voutilainen & Liukkonen, 1995, citados en Hyrkäs et al. (2003).

Ver : <https://www.revistaespacios.com/cited2017/cited2017-23.pdf> entre otra bibliografía.

Firma del Evaluador
DNI-46082806



Anexo N° 4. Validación del instrumento por experto N° 2.

ANEXO

**Validación de instrumento
CARTA DE INVITACIÓN N° 01**

Trujillo, 06 junio de 2023

Dra. Viviane Salli Castillo Benites

Asunto: **Participación en juicio de expertos para validar instrumento de investigación cualitativa**

Me es grato dirigirme a Ud., para expresarle mi respeto y cordial saludo; respecto al asunto hacerle conocer que estoy realizando el trabajo de investigación de enfoque cualitativo titulado: **“Incremento de los delitos informáticos a consecuencia de la pandemia del Covid-19 en la ciudad de Trujillo entre los años 2020-2021 “**

Con el fin de obtener el título de abogado.

La presente investigación tiene por finalidad de determinar si la pandemia del SARS-CoV-2 influyó en el incremento de la delincuencia cibernética en la ciudad de Trujillo; en consecuencia, se deben realizar entrevistas cuyas preguntas conformen el instrumento de evaluación de la presente investigación, que deben ser validadas por expertos, como lo es en el caso de su persona. En ese sentido, **la invitamos a colaborar con la investigación, validando en calidad de experto dicho instrumento de recolección de información.**

Seguros de su participación en calidad de experto para la validación del instrumento de recolección mencionado, se le alcanza el cuestionario de entrevista para su evaluación, adjuntando el formato que servirá para esbozar sus apreciaciones en relación a cada ítem del presente instrumento de investigación. Conocedores de su alto espíritu altruista, agradecemos por adelantado su colaboración.

Atentamente.

Flores Mori Cesar Eugenio
DNI N°47910045

Evaluación por juicio de expertos

Respetado juez: Usted ha sido seleccionado para evaluar el instrumento "Recolección de datos de la información". La evaluación del instrumento es de gran relevancia para lograr que sea válido y que los resultados obtenidos a partir de este sean utilizados eficientemente; aportando al quehacer psicológico. Agradecemos su valiosa colaboración.

1. Datos generales del juez

Nombre del juez:	Viviane Salli Castillo Benites	
Grado profesional:	Maestría (x)	Doctor ()
Área de formación académica:	Clinica ()	Social ()
	Educativa (x)	Organizacional ()
Áreas de experiencia profesional:		
Institución donde labora:		
Tiempo de experiencia profesional en el área:	2 a 4 años (x)	Más de 5 años ()
Experiencia en Investigación Psicométrica: (si corresponde)	Trabajo(s) psicométricos realizados Título del estudio realizado.	

2. Propósito de la evaluación:

Validar el contenido del instrumento, por juicio de expertos.

3. Datos de la escala:

Nombre de la Prueba:	Entrevista
Autores:	Flores Mori Cesar Eugenio
Procedencia:	Propia
Administración:	
Tiempo de aplicación:	
Ámbito de aplicación:	Ciudad de Trujillo
Significación:	Explicar Cómo está compuesta la escala (dimensiones, áreas, ítems por área, explicación breve de cuál es el objetivo de medición)



4. Soporte teórico:

Categorías	Subcategorías	Definición
Ley N° 30096 – Ley de delitos informáticos	<ul style="list-style-type: none"> - Acceso ilícito a datos y sistemas informáticos - Fraude informático - Suplantación de identidad 	Los delitos informáticos implican la utilización de las tecnologías de la información para atentar contra el patrimonio, la fe pública y el mercado financiero. La legislación penal debe adaptarse al desarrollo de la tecnología, lo cual permitirá combatir la ciberdelincuencia. Perú es considerado un país con alta vulnerabilidad ante ataques cibernéticos.
La pandemia del coronavirus en el año 2020 y el dinero digital	<ul style="list-style-type: none"> - ¿Causó el incremento en el uso de la moneda digital? - ¿O en realidad las plataformas digitales bancarias adolecen de medidas de ciberseguridad? 	En el mercado bancario y financiero, es importante que toda operación esté dotada de eficacia y dinamismo. A raíz de la declaración de emergencia sanitaria producto del virus SARS-CoV-2 (Covid-19), los seres humanos evitamos la manipulación de monedas y billetes, con el propósito de contrarrestar los contagios masivos. Ante ello, las entidades monetarias impulsaron el uso de plataformas digitales de pago (Yape, Plin, Tunki, etcétera), lo cual revolucionó el mercado y su uso se volvió obligatorio para realizar negocios con mayor facilidad (o como dicen los comerciales en la televisión: “Haz negocios desde el mueble de tu casa”).

5. Presentación de instrucciones para el juez:

A continuación, a usted le presento el instrumento de recolección de datos elaborado por: Flores Mori Cesar Eugenio en el año 2023. De acuerdo con los siguientes indicadores califique cada uno de los ítems según corresponda

Categoría	Calificación	Indicador
CLARIDAD El ítem se comprende fácilmente, es decir, su sintáctica y semántica son adecuadas.	1. No cumple con el criterio	El ítem no es claro.
	2. Bajo Nivel	El ítem requiere bastantes modificaciones o una modificación muy grande en el uso de las palabras de acuerdo con su significado o por la ordenación de estas.
	3. Moderado nivel	Se requiere una modificación muy específica de algunos de los términos del ítem.
	4. Alto nivel	El ítem es claro, tiene semántica y sintaxis adecuada.
COHERENCIA El ítem tiene relación lógica con la dimensión o indicador que está midiendo.	1. totalmente en desacuerdo (no cumple con el criterio)	El ítem no tiene relación lógica con la dimensión.
	2. Desacuerdo (bajo nivel de acuerdo)	El ítem tiene una relación tangencial /lejana con la dimensión.
	3. Acuerdo (moderado nivel)	El ítem tiene una relación moderada con la dimensión que se está midiendo.
	4. Totalmente de Acuerdo (alto nivel)	El ítem se encuentra está relacionado con la dimensión que está midiendo.
RELEVANCIA El ítem es esencial o importante, es	1. No cumple con el criterio	El ítem puede ser eliminado sin que se vea afectada la medición de la dimensión.
	2. Bajo Nivel	El ítem tiene alguna relevancia, pero otro ítem puede estar incluyendo lo que mide éste.

decir debe ser incluido.	3. Moderado nivel	El ítem es relativamente importante.
	4. Alto nivel	El ítem es muy relevante y debe ser incluido.

Leer con detenimiento los ítems y calificar en una escala de 1 a 4 su valoración, así como solicitamos brinde sus observaciones que considere pertinente

1 no cumple con el criterio
2. Bajo Nivel
3. Moderado nivel
4. Alto nivel

Dimensiones del instrumento:

- Primera dimensión:
Título: Incremento de los delitos informáticos a consecuencia de la pandemia del Covid-19 en la ciudad de Trujillo entre los años 2020-2021
- Objetivos específico: Identificar qué tipo de modalidades de delincuencia cibernética se dieron con más frecuencia en Trujillo 2020-2021.
- Categoría: Incremento de los delitos informáticos.

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
Situaciones adversas	¿Cuáles son los delitos en materia de ciberdelincuencia que tuvieron más incidencia en la ciudad de Trujillo entre el año 2020-2021?	4	3	3	
Objetivo	¿Qué acciones se realizaron para combatir la ciberdelincuencia en la ciudad de Trujillo en los años 2020-2021? ¿Cuál fue el rol de las entidades bancarias/financieras para la búsqueda de soluciones en los delitos de ciberdelincuencia?	4	3	3	

Procedimiento	<p>¿Qué tan difícil han sido identificar a los autores de los delitos de ciberdelincuencia en la ciudad de Trujillo 2020-2021?</p> <p>¿En la actualidad, cuantos casos de delitos informáticos se encuentran en una etapa de juzgamiento en la ciudad de Trujillo en los años 2020-2021?</p> <p>¿Qué mecanismos o procedimientos faltan para una adecuada investigación en los delitos de ciberdelincuencia?</p>	4	3	3	
---------------	--	---	---	---	--

- Segunda dimensión: Desarrollar las soluciones, alternativas y su incidencia en la actividad cibercriminal
- Objetivos 3 de la Dimensión: Desarrollar las alternativas de solución para los delitos de ciberdelincuencias en Trujillo 2020-2021.

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
Modalidades de ciberdelincuencia	¿Resultaría necesario la creación de una fiscalía especializada en ciberdelincuencia en la ciudad de Trujillo? ¿Por qué?	4	3	3	
Causas de la Ciberdelincuencia	¿En qué capacitaciones a participado en relación a los delitos informáticos en el año 2020-2021 en la ciudad de Trujillo?	4	3	3	
Incremento de la Ciberdelincuencia	¿Qué logística le brindo su institución para combatir el incremento de los delitos informáticos en la ciudad de Trujillo en los años 2020-2021?	4	3	3	

Pd.: el presente formato debe tomar en cuenta:

Williams y Webb (1994) así como Powell (2003), mencionan que no existe un consenso respecto al número de expertos a emplear. Por otra parte, el número de jueces que se debe emplear en un juicio depende del nivel de experticia y de la diversidad del conocimiento. Así, mientras Gable y Wolf (1993), Grant y Davis (1997), y Lynn (1986) (citados en McGartland et al. 2003) sugieren un rango de **2** hasta **20 expertos**, Hyrkäs et al. (2003) manifiestan que **10 expertos** brindarán una estimación confiable de la validez de contenido de un instrumento (cantidad mínimamente recomendable para construcciones de nuevos instrumentos). Si un 80 % de los expertos han estado de acuerdo con la validez de un ítem éste puede ser incorporado al instrumento (Voutilainen & Liukkonen, 1995, citados en Hyrkäs et al. (2003).

Ver : <https://www.revistaespacios.com/cited2017/cited2017-23.pdf> entre otra bibliografía.



Viviane Salli Castillo Benites

Firma del Evaluador

DNI: 18191054

Anexo N° 5. Validación del instrumento por experto N° 3.

ANEXO

Validación de instrumento CARTA DE INVITACIÓN N° 01

Trujillo, 06 de junio 2023

Dr. Salinas Ruiz Henry Eduardo

Asunto: **Participación en juicio de expertos para validar instrumento de investigación cualitativa**

Me es grato dirigirme a Ud., para expresarle mi respeto y cordial saludo; respecto al asunto hacerle conocer que estoy realizando el trabajo de investigación de enfoque cualitativo titulado: **“Incremento de los delitos informáticos a consecuencia de la pandemia del Covid-19 en la ciudad de Trujillo entre los años 2020-2021 “**

Con el fin de obtener el título de abogado.

La presente investigación tiene por finalidad de determinar si la pandemia del SARS-CoV-2 influyó en el incremento de la delincuencia cibernética en la ciudad de Trujillo; en consecuencia, se deben realizar entrevistas cuyas preguntas conformen el instrumento de evaluación de la presente investigación, que deben ser validadas por expertos, como lo es en el caso de su persona. En ese sentido, **la invitamos a colaborar con la investigación, validando en calidad de experto dicho instrumento de recolección de información.**

Seguros de su participación en calidad de experto para la validación del instrumento de recolección mencionado, se le alcanza el cuestionario de entrevista para su evaluación, adjuntando el formato que servirá para esbozar sus apreciaciones en relación a cada ítem del presente instrumento de investigación. Conocedores de su alto espíritu altruista, agradecemos por adelantado su colaboración.

Atentamente.



Flores Mori Cesar Eugenio
DNI N°47910045

Evaluación por juicio de expertos

Respetado juez: Usted ha sido seleccionado para evaluar el instrumento "Recolección de datos de la información". La evaluación del instrumento es de gran relevancia para lograr que sea válido y que los resultados obtenidos a partir de este sean utilizados eficientemente; aportando al quehacer psicológico. Agradecemos su valiosa colaboración.

6. Datos generales del juez

Nombre del juez:	Henry Eduardo Salinas Ruiz		
Grado profesional:	Maestría ()	Doctor	(x)
Área de formación académica:	Clínica ()	Social	(x)
	Educativa (x)	Organizacional	(x)
Áreas de experiencia profesional:	Derecho		
Institución donde labora:			
Tiempo de experiencia profesional en el área:	2 a 4 años ()	Más de 5 años	(x)
Experiencia en Investigación Psicométrica: (si corresponde)	Trabajo(s) psicométricos realizados Título del estudio realizado.		

7. Propósito de la evaluación:

Validar el contenido del instrumento, por juicio de expertos.

8. Datos de la escala:

Nombre de la Prueba:	Entrevista
Autores:	Flores Mori Cesar Eugenio Ruiz Guzmán José Ernesto
Procedencia:	Propia
Administración:	
Tiempo de aplicación:	
Ámbito de aplicación:	Ciudad de Trujillo
Significación:	Explicar Cómo está compuesta la escala (dimensiones, áreas, ítems por área, explicación breve de cuál es el objetivo de medición)

9. Soporte teórico:

Categorías	Subcategorías	Definición
Ley N° 30096 – Ley de delitos informáticos	<ul style="list-style-type: none"> - Acceso ilícito a datos y sistemas informáticos - Fraude informático - Suplantación de identidad 	Los delitos informáticos implican la utilización de las tecnologías de la información para atentar contra el patrimonio, la fe pública y el mercado financiero. La legislación penal debe adaptarse al desarrollo de la tecnología, lo cual permitirá combatir la ciberdelincuencia. Perú es considerado un país con alta vulnerabilidad ante ataques cibernéticos.
La pandemia del coronavirus en el año 2020 y el dinero digital	<ul style="list-style-type: none"> - ¿Causó el incremento en el uso de la moneda digital? - ¿O en realidad las plataformas digitales bancarias adolecen de medidas de ciberseguridad? 	En el mercado bancario y financiero, es importante que toda operación esté dotada de eficacia y dinamismo. A raíz de la declaratoria de emergencia sanitaria producto del virus SARS-CoV-2 (Covid-19), los seres humanos evitamos la manipulación de monedas y billetes, con el propósito de contrarrestar los contagios masivos. Ante ello, las entidades monetarias impulsaron el uso de plataformas digitales de pago (Yape, Plin, Tunki, etcétera), lo cual revolucionó el mercado y su uso se volvió obligatorio para realizar negocios con mayor facilidad (o como dicen los comerciales en la televisión: “Haz negocios desde el mueble de tu casa”).

10. Presentación de instrucciones para el juez:

A continuación, a usted le presento el instrumento de recolección de datos elaborado por: Flores Mori Cesar Eugenio y Ruiz Guzmán José Ernesto en el año 2023. De acuerdo con los siguientes indicadores califique cada uno de los ítems según corresponda

Categoría	Calificación	Indicador
CLARIDAD El ítem se comprende fácilmente, es decir, su sintáctica y semántica son adecuadas.	1. No cumple con el criterio	El ítem no es claro.
	2. Bajo Nivel	El ítem requiere bastantes modificaciones o una modificación muy grande en el uso de las palabras de acuerdo con su significado o por la ordenación de estas.
	3. Moderado nivel	Se requiere una modificación muy específica de algunos de los términos del ítem.
	4. Alto nivel	El ítem es claro, tiene semántica y sintaxis adecuada.
COHERENCIA El ítem tiene relación lógica con la dimensión o indicador que está midiendo.	1. totalmente en desacuerdo (no cumple con el criterio)	El ítem no tiene relación lógica con la dimensión.
	2. Desacuerdo (bajo nivel de acuerdo)	El ítem tiene una relación tangencial /lejana con la dimensión.
	3. Acuerdo (moderado nivel)	El ítem tiene una relación moderada con la dimensión que se está midiendo.
	4. Totalmente de Acuerdo (alto nivel)	El ítem se encuentra está relacionado con la dimensión que está midiendo.
	1. No cumple con el criterio	El ítem puede ser eliminado sin que se vea afectada la medición de la dimensión.

RELEVANCIA El ítem es esencial o importante, es decir debe ser incluido.	2. Bajo Nivel	El ítem tiene alguna relevancia, pero otro ítem puede estar incluyendo lo que mide éste.
	3. Moderado nivel	El ítem es relativamente importante.
	4. Alto nivel	El ítem es muy relevante y debe ser incluido.

Leer con detenimiento los ítems y calificar en una escala de 1 a 4 su valoración, así como solicitamos brinde sus observaciones que considere pertinente

1 No cumple con el criterio
2. Bajo Nivel
3. Moderado nivel
4. Alto nivel

Dimensiones del instrumento:

- Primera dimensión:
Título: Incremento de los delitos informáticos a consecuencia de la pandemia del Covid-19 en la ciudad de Trujillo entre los años 2020-2021
- Objetivos específico: Identificar qué tipo de modalidades de delincuencia cibernética se dieron con más frecuencia en Trujillo 2020-2021.
- Categoría: Incremento de los delitos informáticos.

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
Situaciones adversas	¿Cuáles son los delitos en materia de ciberdelincuencia que tuvieron más incidencia en la ciudad de Trujillo entre el año 2020-2021?	4	4	4	
Objetivo	¿Qué acciones se realizaron para combatir la ciberdelincuencia en la ciudad de Trujillo en los años 2020-2021? ¿Cuál fue el rol de las entidades bancarias/financieras para la búsqueda de soluciones en los delitos de ciberdelincuencia?	4	4	4	

Procedimiento	¿Qué tan difícil han sido identificar a los autores de los delitos de ciberdelincuencia en la ciudad de Trujillo 2020-2021?	4	4	4	
	¿En la actualidad, cuantos casos de delitos informáticos se encuentran en una etapa de juzgamiento en la ciudad de Trujillo en los años 2020-2021?				
	¿Qué mecanismos o procedimientos faltan para una adecuada investigación en los delitos de ciberdelincuencia?				

- Segunda dimensión: Desarrollar las soluciones, alternativas y su incidencia en la actividad cibercriminal
- Objetivos 3 de la Dimensión: Desarrollar las alternativas de solución para los delitos de ciberdelincuencias en Trujillo 2020-2021.

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
Modalidades de ciberdelincuencia	¿Resultaría necesario la creación de una fiscalía especializada en ciberdelincuencia en la ciudad de Trujillo? ¿por qué?	4	4	4	
Causas de la Ciberdelincuencia	¿En qué capacitaciones a participado en relación a los delitos informáticos en el año 2020-2021 en la ciudad de Trujillo?	4	4	4	
Incremento de la Ciberdelincuencia	¿Qué logística le brindo su institución para combatir el incremento de los delitos informáticos en la ciudad de Trujillo en los años 2020-2021?	4	4	4	

Pd.: el presente formato debe tomar en cuenta:

Williams y Webb (1994) así como Powell (2003), mencionan que no existe un consenso respecto al número de expertos a emplear. Por otra parte, el número de jueces que se debe emplear en un juicio depende del nivel de experticia y de la diversidad del conocimiento. Así, mientras Gable y Wolf (1993), Grant y Davis (1997), y Lynn (1986) (citados en McGartland et al. 2003) sugieren un rango de **2** hasta **20 expertos**, Hyrkäs et al. (2003) manifiestan que **10 expertos** brindarán una estimación confiable de la validez de contenido de un instrumento (cantidad mínimamente recomendable para construcciones de nuevos instrumentos). Si un 80 % de los expertos han estado de acuerdo con la validez de un ítem éste puede ser incorporado al instrumento (Voutilainen & Liukkonen, 1995, citados en Hyrkäs et al. (2003).

Ver : <https://www.revistaespacios.com/cited2017/cited2017-23.pdf> entre otra bibliografía.



Firma del Evaluador

DNI 41418250

ANEXO 06 ENTREVISTADOS N° 1



Entrevista

Título: 01

"Incremento de los delitos informáticos a consecuencia de la pandemia del Covid-19 en la ciudad de Trujillo entre los años 2020-2021"

INSTRUCCIONES. Leer minuciosamente cada interrogante y responder desde su experiencia laboral y los conocimientos adquiridos, con claridad y autenticidad, en vista de que, la información obtenida corresponde a los resultados del presente trabajo de investigación, cumpliendo de esa manera los objetivos del mismo.

PREGUNTAS:

OBJETIVO ESPECÍFICO 1: Identificar qué tipo de modalidades de delincuencia cibernética se dieron con más frecuencia en Trujillo 2020-2021.

1. ¿Cuáles son los delitos en materia de ciberdelincuencia que tuvieron más incidencia en la ciudad de Trujillo entre el año 2020-2021??

Los delitos con mayor incidencia en el ministerio público fueron los delitos de suplantación de identidad con un porcentaje del 78% de aumento entre los años 2020-2021 pero también aumentaron los delitos de fraude informático con un porcentaje de 38%

2. ¿Qué acciones se realizaron para combatir la ciberdelincuencia en la ciudad de Trujillo en los años 2020-2021?

Se tomaron las medidas preventivas en la cual se informó mediante la plataforma digital del ministerio público a la sociedad a través de facebook las nuevas modalidades de estafas de los delincuentes.

3. ¿Cuál fue el rol de las entidades bancarias/financieras para la búsqueda de soluciones en los delitos de ciberdelincuencia?

Las entidades financieras y los bancos ofrecieron a los usuarios mecanismos de seguridad como los tokens claves temporales para autorización de montos en las transacciones para evitar algún tipo de robo sistemático por parte de los delincuentes cibernéticos.

4. ¿Qué tan difícil han sido identificar a los autores de los delitos de ciberdelincuencia en la ciudad de Trujillo 2020-2021?



ha sido difícil para el ministerio público combatir con los delincuentes cibernéticos ya que no contamos con herramientas tecnológicas que favorezcan las investigaciones eso nos ha dificultado mucho la identificación de los infractores que usan las redes para delinquir.

5. ¿En la actualidad cuantos casos de delitos informáticos se encuentran en una etapa de juzgamiento en la ciudad de Trujillo en los años 2020-2021?

Por ahora si tenemos casos en etapa de juzgamiento dentro de la fiscalía pero la mayoría está en diligencia preliminar y algunas en investigación preparatoria por la falta de herramientas tecnológicas. Es que no se pueden formalizar muchas denuncias.

6. ¿Qué mecanismos o procedimientos faltan para una adecuada investigación en los delitos de ciberdelincuencia?

El gobierno debe destinar un fondo para la compra de herramientas tecnológicas para así nosotros conforme a nuestra función investigadora usar las mismas herramientas tecnológicas que los infractores y combatir la delincuencia cibernética que está avanzando en nuestro país. ello ayudara a reducir las estas.

OBJETIVO ESPECÍFICO 3: Desarrollar las alternativas de solución para los delitos de ciberdelincuencias en Trujillo 2020-2021.

7. ¿Resultaría necesario la creación de una fiscalía especializada en ciberdelincuencia en la ciudad de Trujillo? ¿por qué?

Claro que si resultaría necesario una sede especializada en delitos informáticos para que pueda favorecer en el esclarecimiento de los hechos delictivos de índole informático y con ayuda de las herramientas necesarias y nueva tecnología se podría dar resultados positivos en la identificación de los autores de estos delitos.

8. ¿Qué capacitaciones a participado o en que capacitaciones a participado en relación a los delitos informáticos en el año 2020-2021 en la ciudad de Trujillo?





En ninguna capacitación por el momento la fiscalía no ha capacitado a su personal encargado de estos delitos pero por mi parte si tengo conocimiento de algunas cosas sobre la ciber delincuencia ya que estas modalidades de delinquir están a la orden del día por lo mismo tenemos que estar nosotros capacitados.

9. ¿Qué logística le brindo su institución para combatir el incremento de los delitos informáticos en la ciudad de Trujillo en los años 2020-2021?

En el ministerio público no me brindaron ninguna logística debido al que el área especializada para este tipo de delitos informáticos está en Lima por ende se puede pedir alguna asesoría externa para poder resolver por el momento este tipo de delitos.

OBSERVACIONES:

Denys Keiko Paul Rivas Rodriguez
FISCAL ADJUNTO PROVINCIAL (P)
FISCALÍA PROVINCIAL MIXTA
CORPORATIVA EL PORVENIR

ANEXO 07 ENTREVISTADOS N° 2



UNIVERSIDAD CÉSAR VALLEJO

Entrevista 02

Título:

"Incremento de los delitos informáticos a consecuencia de la pandemia del Covid-19 en la ciudad de Trujillo entre los años 2020-2021"

INSTRUCCIONES. Leer minuciosamente cada interrogante y responder desde su experiencia laboral y los conocimientos adquiridos, con claridad y autenticidad, en vista de que, la información obtenida corresponde a los resultados del presente trabajo de investigación, cumpliendo de esa manera los objetivos del mismo.

PREGUNTAS:

OBJETIVO ESPECÍFICO 1: Identificar qué tipo de modalidades de delincuencia cibernética se dieron con más frecuencia en Trujillo 2020-2021.

1. ¿Cuáles son los delitos en materia de ciberdelincuencia que tuvieron más incidencia en la ciudad de Trujillo entre el año 2020-2021??

Los delitos con mayor incidencia en el año 2020 en la comarca del Alambro fue el delito de suplantación de identidad y también se produjo algunos delitos informáticos como robos a través de estafas cibernéticas o consecuencia de las plataformas digitales en la cual los afectados del estafa realizan sus pagos por medio de aplicativos digitales x yape.

2. ¿Qué acciones se realizaron para combatir la ciberdelincuencia en la ciudad de Trujillo en los años 2020-2021?

se obtuvo por múltiples acciones para poder contrarrestar las nuevas modalidades de la delincuencia cibernética la cual se está poniendo en práctica diáriso capacitando al personal encargado del área de sistema de la policía para la identificación de los softwares maliciosos y los hackers.

3. ¿Cuál fue el rol de las entidades bancarias/financieras para la búsqueda de soluciones en los delitos de ciberdelincuencia?

Los bancos usan el mecanismo de mensaje de texto para poder advertir a sus clientes de cualquier intento de suplantación de identidad o transacciones que no se generaron por el cliente es o ayuda a disminuir los delitos cibernéticos.

4. ¿Qué tan difícil han sido identificar a los autores de los delitos de ciberdelincuencia en la ciudad de Trujillo 2020-2021?



Escaneado con CamScanner



UNIVERSIDAD CÉSAR VALLEJO,

La identificación de los delincuentes cibernéticos es muy difícil de lograr ya que lastimosamente la PNP no cuenta con herramientas del mismo nivel que los hackers por ende solo nos enfocamos en rastrear las llamadas cuando intentan suplantar la identidad de una persona.

5. ¿En la actualidad cuantos casos de delitos informáticos se encuentran en una etapa de juzgamiento en la ciudad de Trujillo en los años 2020-2021?

En la comiseria tenemos denuncias por delitos informaticos pero no se puede hacer mucho ya que no se cuenta con las herramientas necesarias sin embargo nosotros desiamos a la Divinidad para que puedan cooperar en las investigaciones para determinar la culpabilidad del imputado.

6. ¿Qué mecanismos o procedimientos faltan para una adecuada investigación en los delitos de ciberdelincuencia?

se necesita capacitar a los miembros de la P.N.P así como también al M.P para que tengan conocimientos actuales de como combatir la delincuencia cibernética de todos los ángulos y nos vemos limitados en conocimientos digitales, también debemos contar con tecnología de punta para realizar las investigaciones de manera eficaz.

OBJETIVO ESPECÍFICO 3: Desarrollar las alternativas de solución para los delitos de ciberdelincuencias en Trujillo 2020-2021.

7. ¿Resultaría necesario la creación de una fiscalía especializada en ciberdelincuencia en la ciudad de Trujillo? ¿por qué?

La creación de una sede especializada en delitos informáticos en la ciudad de Trujillo ayudaría a descentralizar la carga que tiene la Divinidad sería de mucha ayuda que gente especializada en el Tema informático colabore con las investigaciones para determinar quién es el actor de los delitos.

8. ¿Qué capacitaciones a participado o en que capacitaciones a participado en relación a los delitos informáticos en el año 2020-2021 en la ciudad de Trujillo?



Escaneado con CamScanner



Por el momento ninguna capacitación debido que la policía nacional del Perú no tiene capacitaciones frecuentemente y sobre todo no tiene conocimiento de delitos informáticos por eso pedimos a nuestra institución que nos pueda capacitar para poder tener un mayor conocimiento de las nuevas modalidades delictivas que existen actualmente.

9. ¿Qué logística le brindo su institución para combatir el incremento de los delitos informáticos en la ciudad de Trujillo en los años 2020-2021?

La policía no tiene logística solamente cumplimos nosotros el trabajo de arrestos si esta en fragancia o recepciones las denuncias de las personas que fueron en este caso de fraudadas como son la suplantación de identidad o el robo sistemático de informaciones de cuentas bancarias.

OBSERVACIONES:

S2 P.N.P. Ramírez Ladros
Jennifer Juleisy
CIP N° 31776271



ANEXO 08 ENTREVISTADOS N°3



Entrevista 03

Título:

“Incremento de los delitos informáticos a consecuencia de la pandemia del Covid-19 en la ciudad de Trujillo entre los años 2020-2021”

INSTRUCCIONES. Leer minuciosamente cada interrogante y responder desde su experiencia laboral y los conocimientos adquiridos, con claridad y autenticidad, en vista de que, la información obtenida corresponde a los resultados del presente trabajo de investigación, cumpliendo de esa manera los objetivos del mismo.

PREGUNTAS:

OBJETIVO ESPECÍFICO 1: Identificar qué tipo de modalidades de delincuencia cibernética se dieron con más frecuencia en Trujillo 2020-2021.

1. ¿Cuáles son los delitos en materia de ciberdelincuencia que tuvieron más incidencia en la ciudad de Trujillo entre el año 2020-2021??

Delitos de estafa, apropiación ilícita, hurto (delitos contra el patrimonio) en la modalidad de hurto agravado.

2. ¿Qué acciones se realizaron para combatir la ciberdelincuencia en la ciudad de Trujillo en los años 2020-2021?

Acciones de prevención, cursos de talleres y capacitaciones, todo ello en coordinación de la Policía Nacional del Perú a efectos de combatir la ciberdelincuencia, que dichos actos cometidos por personas de mal vivir se viene arraizando cada vez más en nuestra sociedad.

3. ¿Cuál fue el rol de las entidades bancarias/financieras para la búsqueda de soluciones en los delitos de ciberdelincuencia?

El rol de las empresas financieras fueron de devolver el dinero a los agraviados, las mismas que contaban con seguro.

4. ¿Qué tan difícil han sido identificar a los autores de los delitos de ciberdelincuencia en la ciudad de Trujillo 2020-2021?





La identificación plena de los autores de estos delitos ha sido previa a una investigación minuciosa.

5. ¿En la actualidad cuantos casos de delitos informáticos se encuentran en una etapa de juzgamiento en la ciudad de Trujillo en los años 2020-2021?

En la etapa de juicio oral existen 20 casos.

6. ¿Qué mecanismos o procedimientos faltan para una adecuada investigación en los delitos de ciberdelincuencia?

Mayor logística y apoyo por parte de El Estado, esto es mayor capacitación al personal, y asimismo los entes de El Estado deben trabajar en conjunto.

OBJETIVO ESPECÍFICO 3: Desarrollar las alternativas de solución para los delitos de ciberdelincuencias en Trujillo 2020-2021.

7. ¿Resultaría necesario la creación de una fiscalía especializada en ciberdelincuencia en la ciudad de Trujillo? ¿por qué?

Sí, porque se tendría un rol de especialidad quienes deben de realizar una mejor investigación en conjunto con la policía.

8. ¿Qué capacitaciones a participado o en que capacitaciones a participado en relación a los delitos informáticos en el año 2020-2021 en la ciudad de Trujillo?



Solo nos brindan folletos de las nuevas tecnologías que utilizan los ciber delinuentes pero no participe en ninguna capacitación por que mi institución no las brinda limitando así nuestro trabajo a diario ya que a veces se pueda hacer muchas cosas pero con la tecnología que tenemos no se puede hacer nada solamente realizar la investigación pertinente.

9. ¿Qué logística le brinda su institución para combatir el incremento de los delitos informáticos en la ciudad de Trujillo en los años 2020-2021?

Acceso a diversas plataformas de internet con las instituciones públicas, a fin de poder identificar a los presuntos responsables de los hechos delictivos.

OBSERVACIONES:

Helder Cochachin
Ramirez

DNI : 31655749

ANEXO 09 ENTREVISTADOS N°4



UNIVERSIDAD CÉSAR VALLEJO

Entrevista 04

Título:

“Incremento de los delitos informáticos a consecuencia de la pandemia del Covid-19 en la ciudad de Trujillo entre los años 2020-2021”

INSTRUCCIONES. Leer minuciosamente cada interrogante y responder desde su experiencia laboral y los conocimientos adquiridos, con claridad y autenticidad, en vista de que, la información obtenida corresponde a los resultados del presente trabajo de investigación, cumpliendo de esa manera los objetivos del mismo.

PREGUNTAS:

OBJETIVO ESPECÍFICO 1: Identificar qué tipo de modalidades de delincuencia cibernética se dieron con más frecuencia en Trujillo 2020-2021.

1. ¿Cuáles son los delitos en materia de ciberdelincuencia que tuvieron más incidencia en la ciudad de Trujillo entre el año 2020-2021??

Las denuncias recibidas en la comisaría del Alambre muestran que el delito de suplantación de identidad tiene un mayor porcentaje sobre todos los delitos de ciberdelincuencia en el 2020-2021

2. ¿Qué acciones se realizaron para combatir la ciberdelincuencia en la ciudad de Trujillo en los años 2020-2021?

tomamos la iniciativa de brindar charlas informativas con relación a los delitos informáticos para educar a la población a no caer en el error de ingresar a páginas desconocidas o ser víctimas de suplantación de identidad.

3. ¿Cuál fue el rol de las entidades bancarias/financieras para la búsqueda de soluciones en los delitos de ciberdelincuencia?

Las entidades bancarias desarrollaron aplicativos oficiales como B.C.P móvil, tunki billetera digital etc para brindar seguridad al momento de realizar operaciones bancarias a su vez también atendió algunos pequeños imperfectos en el aplicativo.

4. ¿Qué tan difícil han sido identificar a los autores de los delitos de ciberdelincuencia en la ciudad de Trujillo 2020-2021?



Escaneado con CamScanner



muchas veces es difícil identificar a los autores de los ciberdelitos ya que en primer lugar no se cuenta con las mismas herramientas tecnológicas necesarias y a su vez el personal no está capacitado para poder realizar las investigaciones correspondientes.

5. ¿En la actualidad cuantos casos de delitos informáticos se encuentran en una etapa de juzgamiento en la ciudad de Trujillo en los años 2020-2021?

por el momento el Ministerio Público ha informado en que estado se encuentra dichas denuncias ya que están en etapa de investigación preparatoria. es decir sigue en investigaciones para determinar a los autores y así poder sancionarlos.

6. ¿Qué mecanismos o procedimientos faltan para una adecuada investigación en los delitos de ciberdelincuencia?

para realizar una adecuada investigación debemos contar únicamente con herramientas tecnológicas mucho más avanzadas que los delincuentes para con ello combatirlos porque sin las herramientas necesarias no se puede hacer mucho para identificar a los delincuentes ni mucho menos para continuar las investigaciones esto dificulta la tarea de la P.N.P

OBJETIVO ESPECÍFICO 3: Desarrollar las alternativas de solución para los delitos de ciberdelincuencias en Trujillo 2020-2021.

7. ¿Resultaría necesario la creación de una fiscalía especializada en ciberdelincuencia en la ciudad de Trujillo? ¿por qué?

Si resultaría muy necesaria la creación de una sede fiscal como la capital que tiene una fiscalía especializada en delitos informáticos en Lima centro donde se puede tener mayor enfoque al momento de llevar este tipo de casos ya que en la actualidad en la ciudad de Trujillo no tenemos las herramientas necesarias para combatir este tipo de ilícitos.

8. ¿Qué capacitaciones a participado o en que capacitaciones a participado en relación a los delitos informáticos en el año 2020-2021 en la ciudad de Trujillo?





No por el momento no tengo conocimiento de que en los años 2020-2021 se estuviera brindando algún tipo de capacitación y eso que el nivel de ciberdelitos aumento debido a la pandemia del covid 19 pero la mayoría de personas estafadas por las redes sociales su denuncia no progresa debido a que la policía no está capacitada para hacer el rastreo de los delitos cibernéticos.

9. ¿Qué logística le brinda su institución para combatir el incremento de los delitos informáticos en la ciudad de Trujillo en los años 2020-2021?

No, ningún tipo de apoyo me brinda la policía debido a que la policía solo recepciona las denuncias pero no las investigan a fondo solamente tenemos que limitarnos a ciertas cosas y no podemos investigar mas me gustaria pertenecer a otras areas como la Divinidad.

OBSERVACIONES:

S1 PNP PEREZ BURGOS
OMAR JHONATAN
CIP N° 31685795

ANEXO 10 ENTREVISTADOS N°5



UNIVERSIDAD CÉSAR VALLEJO

Entrevista 05

Título:

"Incremento de los delitos informáticos a consecuencia de la pandemia del Covid-19 en la ciudad de Trujillo entre los años 2020-2021"

INSTRUCCIONES. Leer minuciosamente cada interrogante y responder desde su experiencia laboral y los conocimientos adquiridos, con claridad y autenticidad, en vista de que, la información obtenida corresponde a los resultados del presente trabajo de investigación, cumpliendo de esa manera los objetivos del mismo.

PREGUNTAS:

OBJETIVO ESPECÍFICO 1: Identificar qué tipo de modalidades de delincuencia cibernética se dieron con más frecuencia en Trujillo 2020-2021.

1. ¿Cuáles son los delitos en materia de ciberdelincuencia que tuvieron más incidencia en la ciudad de Trujillo entre el año 2020-2021??
Las denuncias con mayor incidencia han sido las suplantación de identidad y también las estafas cibernéticas como el gota a gota.
2. ¿Qué acciones se realizaron para combatir la ciberdelincuencia en la ciudad de Trujillo en los años 2020-2021?
Con supervisión de mi comandante de la comisaría de Bellavista fuimos a distintos puntos para ayudar a la gente a cobrar sus respectivos bonos y evitar que sean víctimas de la delincuencia cibernética.
3. ¿Cuál fue el rol de las entidades bancarias/financieras para la búsqueda de soluciones en los delitos de ciberdelincuencia?
Los bancos usaron el mecanismo de alertas a la población mediante mensajes de texto manifestando que ellos no solicitan información personal a los usuarios ya que cualquier trámite es de manera personal y portando su D.N.I
4. ¿Qué tan difícil han sido identificar a los autores de los delitos de ciberdelincuencia en la ciudad de Trujillo 2020-2021?





Es difícil para nosotros como policías no saber como actuar frente a estos delitos tecnológicos que cada día avanzan y superan expectativas e identificar a quienes delinquen es una tarea casi imposible

5. ¿En la actualidad cuantos casos de delitos informáticos se encuentran en una etapa de juzgamiento en la ciudad de Trujillo en los años 2020-2021?

En nuestra comiseria hemos recibido denuncias sobre delitos informáticos los cuales comunicamos al M.P. para las investigaciones correspondientes sin embargo no se tiene noticias aun de que dichos casos estén en etapa de juzgamiento.

6. ¿Qué mecanismos o procedimientos faltan para una adecuada investigación en los delitos de ciberdelincuencia?

para nosotros realizar las investigaciones de los contra los delitos cibernéticos debemos adquirir herramientas tecnológicas que favorezcan el trabajo seguido a ello necesitamos capacitaciones respecto a la tecnología por que como sabemos este avanza de manera desmesurada.

OBJETIVO ESPECÍFICO 3: Desarrollar las alternativas de solución para los delitos de ciberdelincuencias en Trujillo 2020-2021.

7. ¿Resultaría necesario la creación de una fiscalía especializada en ciberdelincuencia en la ciudad de Trujillo? ¿por qué?

Estoy de acuerdo con el M.P pueda tener mayor conocimiento de los ciberdelitos por eso sería factible la creación de una fiscalia en la ciudad para asi facilitarnos nuestro trabajo como servidores publicos y como la policia realizamos nuestras labores a diario pero vemos que no son suficientes la tecnología que tenemos en nuestra dependencia policial para combatir a los delincuentes.

8. ¿Qué capacitaciones a participado o en que capacitaciones a participado en relación a los delitos informáticos en el año 2020-2021 en la ciudad de Trujillo?



Solamente participe en la universidad en algunas capacitaciones pero en la policía no nos brindan esos mecanismos para poder combatir la ciberdelincuencia si bien es cierto tenemos una división que es la Divindod que significa que combate los delitos de alta tecnología pero la verdad no se da abasto si fuera posible el estado peruano debería invertir en capacitaciones.

9. ¿Qué logística le brindo su institución para combatir el incremento de los delitos informáticos en la ciudad de Trujillo en los años 2020-2021?

Si me brindaron algunos tips para combatir los delitos informáticos pero fueron simples no fue una clase de capacitación fueron algunos tips breves del comisario donde se nos informó como están operando los delincuentes ahora.

OBSERVACIONES:



52 PNA GARCIA SOLIS
ELIANA ELIZABETH
CIP N° 31792463

ANEXO 11 ENTREVISTADOS N°6



Entrevista 06

Título:

"Incremento de los delitos informáticos a consecuencia de la pandemia del Covid-19 en la ciudad de Trujillo entre los años 2020-2021"

INSTRUCCIONES. Leer minuciosamente cada interrogante y responder desde su experiencia laboral y los conocimientos adquiridos, con claridad y autenticidad, en vista de que, la información obtenida corresponde a los resultados del presente trabajo de investigación, cumpliendo de esa manera los objetivos del mismo.

PREGUNTAS:

OBJETIVO ESPECÍFICO 1: Identificar qué tipo de modalidades de delincuencia cibernética se dieron con más frecuencia en Trujillo 2020-2021.

1. ¿Cuáles son los delitos en materia de ciberdelincuencia que tuvieron más incidencia en la ciudad de Trujillo entre el año 2020-2021??

En la comiseria de la Noria las denuncias mas recurrentes fueron las de suplantación de identidad ya que mas afectaron a la población en la época del covid 19 debido a que las personas se registraban para cobrar su bono yanapay y resultaron estafadas.

2. ¿Qué acciones se realizaron para combatir la ciberdelincuencia en la ciudad de Trujillo en los años 2020-2021?

Se realizó una guía para las personas que desconocen el uso adecuado de la tecnología y así evitar una mayor propagación de los ciberdelitos

3. ¿Cuál fue el rol de las entidades bancarias/financieras para la búsqueda de soluciones en los delitos de ciberdelincuencia?

Todos los bancos obtaron por mejorar la seguridad en sus plataformas digitales asiendo que su registro sea mucho mas exhaustivo para asi evitar la suplantación de identidad que es uno de los delitos mas comunes de la localidad.

4. ¿Qué tan difícil han sido identificar a los autores de los delitos de ciberdelincuencia en la ciudad de Trujillo 2020-2021?



La identificación de los delincuentes cibernéticos es un trabajo difícil por que no se cuenta con un presupuesto destinado a mejorar nuestra tecnología para con ello poder solucionar los problemas de la sociedad sin embargo con las pocas herramientas que tenemos

5. ¿En la actualidad cuantos casos de delitos informáticos se encuentran en una etapa de juzgamiento en la ciudad de Trujillo en los años 2020-2021?
conforme la ley 30096 se debe sancionar a los autores que cometan delitos informáticos sin embargo en muchos casos aun no se identifican a los autores, lo que hace imposible sancionarlos.

6. ¿Qué mecanismos o procedimientos faltan para una adecuada investigación en los delitos de ciberdelincuencia?
Falta inversión en la tecnología luego de ello capacitarlos a quienes llevamos las investigaciones en este caso el M.P para poder realizar un trabajo adecuado a su vez realizar pequeñas charlas a la población para que conozca un poco mas y educarse con la tecnología.

OBJETIVO ESPECÍFICO 3: Desarrollar las alternativas de solución para los delitos de ciberdelincuencias en Trujillo 2020-2021.

7. ¿Resultaría necesario la creación de una fiscalía especializada en ciberdelincuencia en la ciudad de Trujillo? ¿por qué?

La verdad que seria grandioso que los representantes del M.P puedan tener una sede en el departamento de la Libertad y no solo en Lima, por eso debería la fiscal de la nación comprometerse con la creación de fiscalías especializadas en ciberdelitos para poder asi combatir el crimen organizado.

8. ¿Qué capacitaciones a participado o en que capacitaciones a participado en relación a los delitos informáticos en el año 2020-2021 en la ciudad de Trujillo?


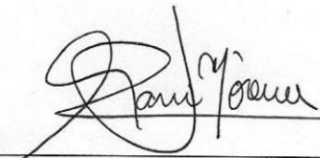


No nunca participe tampoco e visto casos de delitos informáticos pero la verdad es que no tengo el conocimiento para poder investigar más sobre el tema debido a que el M.P. carece mucho de conocimiento de nuevos delitos cibernéticos por los mismos nosotros nos agenciamos de varios videos para poder ver cuales son la nuevas tecnologías delictivas pero la policia no brinda hasta la actualidad, deberia siquiera brindar alguien curso con la finalidad que reduzca la delincuencia informatica en Trujillo

9. ¿Qué logística le brinda su institución para combatir el incremento de los delitos informáticos en la ciudad de Trujillo en los años 2020-2021?

Blaro realizamos muchos operativos con el fin de recepcionar los teléfonos donde operaban los cibercriminales a través de perfiles falsos haciéndose a si de cuantiosas sumas de dinero a través de las estafas por redes sociales por lo mismo nosotros realizamos operativos para corroborar el los IMEI de los celulares si son robados.

OBSERVACIONES:

<p>Abg. María Angélica Rosas Moreno  ABOGADO Reg. CALL. 012402</p>	
<p>Sello</p>	<p>Firma</p>

ANEXO 12 AUTORIZACION DE RECOPIACION DE INFORMACION

UNIVERSIDAD CÉSAR VALLEJO

"Año de la unidad, la paz y el desarrollo"

Trujillo, 06 de Julio de 2023

CARTA N° 010-2023-UCV-VA-P08/DE

REPRESENTANTE DEL MINISTERIO PUBLICO
Coordinación de la Fiscalía mixta corporativa del Porvenir.
Presente.

ASUNTO: AUTORIZACIÓN PARA RECOPIACIÓN DE INFORMACIÓN


Es grato dirigirme a Ud. para saludarle cordialmente y al mismo tiempo presentar al estudiante **FLORES MORI, CESAR EUGENIO**, con DNI N° 47910045, con Código de estudiante N° 7002453326 de la Escuela de **DERECHO** de la Universidad César Vallejo.



El estudiante en mención solicita autorización para recopilar la información necesaria para su trabajo de Investigación titulado: **Incremento de los delitos informáticos a consecuencia de la pandemia del covid-19 en la ciudad de Trujillo entre los años 2020-2021.**, en la institución que Ud. dirige.

El objetivo principal de este trabajo de investigación es Determinar las causales del incremento de delincuencia cibernética en tiempos de aislamiento social obligatorio producto del COVID 19.

Agradeciendo la atención que brinde a la presente, aprovecho la oportunidad para expresarle mi consideración y respeto.

Atentamente,

 **M^g Giuliana Katherine Tirado Gardi**
Coordinadora- Sede Trujillo
Escuela de Derecho UCV


MINISTERIO PUBLICO
FISCALIA PROVINCIAL MIXTA CORPORATIVA
DEL EL PORVENIR
MESA DE
06 JUL 2023
RECIBIDO
Hora 10:30 Firma 

"Año del Bicentenario del Perú: 200 años de Independencia"

Trujillo, 16 de mayo de 2023

CARTA N° 011-2023-UCV-VA-P08/DE

REPRESENTANTE DEL MINISTERIO PÚBLICO

Ministerio público distrito fiscal de la Libertad.

Presente. -

ASUNTO: AUTORIZACIÓN PARA RECOPIACIÓN DE INFORMACIÓN

Es grato dirigirme a Ud. para saludarle cordialmente y al mismo tiempo presentar al estudiante **FLORES MORI, CESAR EUGENIO**, con DNI N° 47910045, con Código de estudiante N° 7002453326 de la Escuela de **DERECHO** de la Universidad César Vallejo.


El estudiante en mención solicita autorización para recopilar la información necesaria para su trabajo de Investigación titulado: **Incremento de los delitos informáticos a consecuencia de la pandemia del covid-19 en la ciudad de Trujillo entre los años 2020-2021.**, en la institución que Ud. dirige.

El objetivo principal de este trabajo de investigación es Determinar las causales del incremento de delincuencia cibernética en tiempos de aislamiento social obligatorio producto del COVID 19.

Agradeciendo la atención que brinde a la presente, aprovecho la oportunidad para expresarle mi consideración y respeto.

Atentamente,




Giuliana Katherine Tirado Garcia
Coordinadora- Sede Trujillo
Escuela de Derecho UCV

"Año del Bicentenario del Perú: 200 años de Independencia"

Trujillo, 16 de mayo de 2023

CARTA N° 013-2023-UCV-VA-P08/DE

REPRESENTANTE DEL MINISTERIO PÚBLICO

Fiscalía del Porvenir.

Presente. -

ASUNTO: AUTORIZACIÓN PARA RECOPIACIÓN DE INFORMACIÓN

Es grato dirigirme a Ud. para saludarle cordialmente y al mismo tiempo presentar al estudiante **FLORES MORI, CESAR EUGENIO**, con DNI N° 47910045, con Código de estudiante N° 7002453326 de la Escuela de **DERECHO** de la Universidad César Vallejo.

El estudiante en mención solicita autorización para recopilar la información necesaria para su trabajo de Investigación titulado: **Incremento de los delitos informáticos a consecuencia de la pandemia del covid-19 en la ciudad de Trujillo entre los años 2020-2021.**, en la institución que Ud. dirige.

El objetivo principal de este trabajo de investigación es Determinar las causales del incremento de delincuencia cibernética en tiempos de aislamiento social obligatorio producto del COVID 19.

Agradeciendo la atención que brinde a la presente, aprovecho la oportunidad para expresarle mi consideración y respeto.

Atentamente,



M^o Giuliana Katherine Tirado Garcia
Coordinadora- Sede Trujillo
Escuela de Derecho UCV

"Año del Bicentenario del Perú: 200 años de Independencia"

Trujillo, 16 de mayo de 2023

CARTA N° 010-2023-UCV-VA-P08/DE

COMANDANTE

COMISARÍA DE AYACUCHO

COMISARÍA DEL ALAMBRE

COMISARÍA DE LA NORIA

COMISARIA DE BELLAVISTA

Presente. -

ASUNTO: AUTORIZACIÓN PARA RECOPIACIÓN DE INFORMACIÓN

Es grato dirigirme a Ud. para saludarle cordialmente y al mismo tiempo presentar al estudiante **FLORES MORI, CESAR EUGENIO**, con DNI N° 47910045, con Código de estudiante N° 7002453326 de la Escuela de **DERECHO** de la Universidad César Vallejo.


El estudiante en mención solicita autorización para recopilar la información necesaria para su trabajo de Investigación titulado: **Incremento de los delitos informáticos a consecuencia de la pandemia del covid-19 en la ciudad de Trujillo entre los años 2020-2021.**, en la institución que Ud. dirige.

El objetivo principal de este trabajo de investigación es Determinar las causales del incremento de delincuencia cibernética en tiempos de aislamiento social obligatorio producto del COVID 19.

Agradeciendo la atención que brinde a la presente, aprovecho la oportunidad para expresarle mi consideración y respeto.

Atentamente,




Giuliana Katherine Tirado Garcia
Coordinadora- Sede Trujillo
Escuela de Derecho UCV

"Año del Bicentenario del Perú: 200 años de Independencia"

Trujillo, 16 de mayo de 2023

CARTA N° 014-2023-UCV-VA-P08/DE

REPRESENTANTE DEL MINISTERIO PÚBLICO

Fiscalía de Trujillo.

Presente. -

ASUNTO: AUTORIZACIÓN PARA RECOPIACIÓN DE INFORMACIÓN

Es grato dirigirme a Ud. para saludarle cordialmente y al mismo tiempo presentar al estudiante **FLORES MORI, CESAR EUGENIO**, con DNI N° 47910045, con Código de estudiante N° 7002453326 de la Escuela de **DERECHO** de la Universidad César Vallejo.

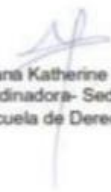
El estudiante en mención solicita autorización para recopilar la información necesaria para su trabajo de Investigación titulado: **Incremento de los delitos informáticos a consecuencia de la pandemia del covid-19 en la ciudad de Trujillo entre los años 2020-2021.**, en la institución que Ud. dirige.

El objetivo principal de este trabajo de investigación es Determinar las causales del incremento de delincuencia cibernética en tiempos de aislamiento social obligatorio producto del COVID 19.

Agradeciendo la atención que brinde a la presente, aprovecho la oportunidad para expresarle mi consideración y respeto.

Atentamente,




Giuliana Katherine Tirado Garcia
Coordinadora- Sede Trujillo
Escuela de Derecho UCV

"Año del Bicentenario del Perú: 200 años de Independencia"

Trujillo, 16 de mayo de 2023

CARTA N° 012-2023-UCV-VA-P08/DE

REPRESENTANTE DEL MINISTERIO PÚBLICO

Fiscalía Provincial mixta de la Esperanza.

Presente. -

ASUNTO: AUTORIZACIÓN PARA RECOPIACIÓN DE INFORMACIÓN

Es grato dirigirme a Ud. para saludarle cordialmente y al mismo tiempo presentar al estudiante **FLORES MORI, CESAR EUGENIO**, con DNI N° 47910045, con Código de estudiante N° 7002453326 de la Escuela de **DERECHO** de la Universidad César Vallejo.


El estudiante en mención solicita autorización para recopilar la información necesaria para su trabajo de Investigación titulado: **Incremento de los delitos informáticos a consecuencia de la pandemia del covid-19 en la ciudad de Trujillo entre los años 2020-2021.**, en la institución que Ud. dirige.

El objetivo principal de este trabajo de investigación es Determinar las causales del incremento de delincuencia cibernética en tiempos de aislamiento social obligatorio producto del COVID 19.

Agradeciendo la atención que brinde a la presente, aprovecho la oportunidad para expresarle mi consideración y respeto.

Atentamente,




Giuliana Katherine Tirado Garcia
Coordinadora- Sede Trujillo
Escuela de Derecho UCV

ANEXO 13
FOTOGRAFIAS DE LOS ENTREVISTADOS





