UNIVERSIDAD ESPECIALIZADA DE LAS AMÉRICAS

Facultad de Educación Social y Desarrollo Humano

Escuela de Educación Social

Trabajo de Grado para Optar por el Título de Licenciado

en

Investigación Criminal y Seguridad

Modalidad

Tesis

Procedimientos en la Investigación Judicial de Estafas a través de medios cibernéticos o informáticos

Presentado por:

Pérez Noriega, Luis Eduardo 2-744-591

Asesor:

Mitzila Lorena Acosta Herrera

Panamá, 2022

DEDICATORIA

Dedico esta investigación a mis familiares que me apoyaron en esta travesía, primordialmente a mis padres, Yamileth Noriega y Luis Pérez, quienes con sus palabras motivadoras y siendo benefactores de la parte económica en estos cuatro años de la carrera.

Para mi hermana, Vanessa Pérez, mi novia, Eleysa González, mi tía, Anayansi Pérez, por brindarme el apoyo emocional y los constantes consejos que fueron pilares muy relevantes para la culminación de este trabajo de grado.

También a mí, por ser un logro personal al culminar esta tesis, brindando conocimientos en el área de investigación de los delitos, aprendizaje que me llena de orgullo.

Luis E. Pérez N.

AGRADECIMIENTO

A todo el personal docente de la Licenciatura de Investigación Criminal y Seguridad de la Universidad Especializada de las Américas (UDELAS), que me han formado como un profesional en la investigación de los delitos y en materia de seguridad.

Agradezco muy especialmente, a los profesores Lineth Flores e Iván Varela quienes me nutrieron con sus conocimientos de la carrera y, además, estuvieron en todos los años de la licenciatura brindándome su incondicional apoyo, también a mi asesora Mitzila Acosta, que sin ella no habría sido posible realizar esta investigación.

En fin, a cada una de las personas que me ayudaron de una u otra forma para alcanzar este gran triunfo.

Luis E. Pérez N.

RESUMEN

La siguiente investigación denominada “Procedimientos de Investigación Judicial de Estafas a través de Medios Cibernéticos o informáticos”, realizada en el Corregimiento de Aguadulce en 2021 y 2022, con objetivos encaminados en analizar los procedimientos utilizados en la investigación de este delito en el corregimiento de Aguadulce, la explicación de este delito y capacidad de las autoridades, así como la percepción de los residentes del lugar.

A través una metodología compuesta por enfoque mixto, de diseño no experimental, y con estudio descriptivo y explicativo, obteniendo una perspectiva amplia y profunda de este delito, igualmente exploratoria, por la inexistencia de un trabajo de grado enfocado en este tema.

Ofreciendo resultados relevantes sobre la capacidad de funcionarios de las instituciones auxiliares de investigación, en este caso conformada por la seccional de la DIJ de Aguadulce y el IMELCF de Los Santos, en su sección de Delitos Informáticos.

Así mismo, está presente la participación de parte de la sociedad en la investigación, conformada por residentes del corregimiento de Aguadulce, conociendo su percepción sobre los procedimientos actualmente utilizados en las investigaciones de este fenómeno delictivo.

Palabras claves: Investigación judicial, Procedimiento de investigación, Delitos Informáticos, Ciberestafa, Estafa informática, Estafa en línea, Estafa tecnológica.

ABSTRACT

The following research called "Judicial Investigation Procedures of Swindles through cybernetic or computer media", carried out in Aguadulce in 2021 and 2022, with objectives aimed at analyzing the procedures used in the investigation of this crime in Aguadulce, the explanation of this crime and the capacity of the authorities, as well as the perception of the residents of the place.

Through a methodology composed by a mixed approach, non-experimental design, with a descriptive and explanatory study, obtaining a wide and deep perspective of this crime, also exploratory, due to the inexistence of a degree work focused on this topic.

Offering relevant results on the capacity of officials of the auxiliary investigation institutions, in this case formed by the Aguadulce branch of the DIJ and the IMELCF of Los Santos, in its Computer Crimes section.

Likewise, the participation of part of the society in the investigation is present, made up of residents of Aguadulce, knowing their perception of the procedures currently used in the investigations of this criminal phenomenon.

Key words: Judicial investigation, Investigation procedure, Computer crimes, Cyber swindle, Computer swindle, Online swindle, Technological swindle.

CONTENIDO GENERAL

Página

INTRODUCCIÓN

Los procedimientos de los nuevos delitos cometidos por medio de las tecnologías de información y comunicación son relevantes en la resolución de este tipo de ilícito, ya que, establecen un protocolo específico que utilizan los investigadores y criminalística, haciendo que su labor sea eficiente.

Debido a un aumento exponencial en las diferentes modalidades de las estafas a través de medios cibernéticos o informáticos a nivel mundial, y principalmente en países en donde las políticas criminales dirigidas a contrarrestar este delito son ineficaces o inexistentes, establecer una serie de pasos y principios beneficiará a la investigación.

Nuestro país no escapa de esta realidad y menos en sectores en donde la inversión a las instituciones o cuerpo de investigación es menor, por esto, la presente investigación realizada en el corregimiento de Aguadulce en los años 2021 y 2022, cuyo tema es “Procedimientos de Investigación Judicial de Estafas a través Medios Cibernéticos o Informáticos”, se centra en recabar información sobre los metodos utilizados en la actualidad, así como la perspectiva de los residentes sobre este fenómeno delictivo.

En ese sentido el presente trabajo de investigación, se estructura por cuatro capítulos expuestos de la siguiente forma:

El capítulo I, denominado “Aspectos generales de la investigación”, estará conformado por el planteamiento de la investigación, formado por los antecedentes teóricos de diversos autores, la situación actual, el problema de la investigación, así mismo, su justificación, hipótesis y los objetivos planteados para este estudio.

En el capítulo II, denominado “Marco teórico”, se establecen nociones generales y específicas sobre el tema, con el fin de respaldar la investigación con diversas teorías y análisis sobres esta conducta delictiva. Algunos de los puntos son los procedimientos de investigación con los pasos y principios, el ciberdelito, el ciberespacio, las nuevas técnicas de investigación, las víctimas y victimarios y las instituciones panameñas de investigación para los ciberdelitos.

Un punto destacado en este capítulo es la estafa tradicional y su normativa actual, hasta llegar a las estafas a través de medios cibernéticos o informáticos, textualizando las diferentes modalidades; mostrando las ventajas del ciberestafador, su dinámica, así como las complicaciones en la investigación de estos hechos.

En el capítulo III, denominado “Marco metodológico”, se muestra el enfoque de la investigación, el diseño y tipo de estudio, la población, las muestras y el tipo de muestreo, las variables con las definiciones conceptuales y operacionales, las técnicas e instrumentos de recolección de los datos y los procedimientos realizados en la investigación.

En tanto, en el capítulo IV, denominado “Análisis y discusión de los resultados”, se presentan los datos obtenidos de las técnicas e instrumentos aplicados, realizando la interpretación y el análisis de los mismos, para poder plantear las conclusiones y recomendaciones en relación al tema en estudio, exponiendo también las limitaciones presentadas durante el desarrollo de la investigación.

Finalmente, se detallan las referencias bibliográficas e infográficas consultadas, así como los anexos pertinentes.

CAPÍTULO I

CAPÍTULO I: ASPECTOS GENERALES DE LA INVESTIGACIÓN

1.1 Planteamiento del problema

En la era de la informática los diferentes equipos de tecnologías innovadoras como las calculadoras electrónicas, funcionales y con gran capacidad, solo han quedado vestigios de las primeras máquinas de cómputo, afectando en gran medida nuestras actividades cotidianas, para ser controladas de forma directa e indirecta, así mismo presentes en sectores de mucha relevancia para la organización de un estado, como la educación, el transporte, el tráfico aéreo, etc., dependiendo de las computadoras (Gutiérrez, 2015).

Córtez, Haydee y Lagos (2020) afirman:

> **La evolución de la tecnología ha permitido que el ser humano acceda a medios de comunicación, antes inimaginables. Sin embargo, la internet sea convertido en centro de operaciones para muchas conductas desviadas criminales, quienes aprovechan la "fragilidad" de los sistemas de seguridad de la mayoría de los cibernautas, consiguiendo apoderarse de información personal y, en la mayoría de los casos, apoderarse de recursos patrimoniales que perjudican a sus verdaderos propietarios.** (p.180)

El internet ha permitido reducir el tiempo de espera en las diferentes actividades, un ejemplo de estos sería la espera de un banco, en la actualidad el uso de aplicaciones como la banca móvil o en línea, si bien ha traído ventajas por la comodidad que representa; pero la misma es beneficiosa para el delincuente a no requerir un arma o poner su vida en riesgo para ingresar al banco y sustraer el bien ajeno (Beermann, 2018).

> **Las amenazas y peligros que nos rodean avanzan igual que lo hacen las sociedades, por ello, la seguridad ha supuesto últimamente un auge en las agendas de las políticas públicas por los problemas derivados del nuevo terrorismo, la globalización, la sofisticación de la delincuencia, la excesiva brutalidad de las nuevas y diversas figuras delictivas, en definitiva, por el creciente aumento de la inseguridad ciudadana. Las diferentes policías son las encargadas directamente de evitar que estas amenazas y peligros no se lleven a cabo. Al igual que la sociedad ha ido evolucionando y cambiando, las policías lo han hecho adaptándose a los acontecimientos para poder ofrecer el mejor servicio a los ciudadanos.** (Carque, 2016, p.45).

Las técnicas de investigación tradicionales son claramente insuficientes para investigar los ciberdelitos, debido a que los procedimientos utilizados tradicionalmente no tienen regulaciones necesarias para la investigación de este tipo de conductas ilícitas. Con la influencia del internet en la criminalidad, por generar nuevas formas de actuar y con aumento en los delitos tradicionales, denominadas estas nuevas conductas o modificaciones de comportamientos tradicionales como ciberdelito, donde las investigaciones exigen conocer técnicas básicas de internet, es decir saber cómo funciona este entorno y los diversos dispositivos que conforman esta red (Quevedo, 2017).

De acuerdo con Leal (2011) en los procedimientos de investigación de un delito, el transcurso del tiempo juega un papel fundamental para la impunidad del delincuente, con solo 24 horas de haber realizado el acto delictivo es vital obtener indicios.

Sin embargo, existen dificultades para resolver los delitos con el uso de tecnologías informáticas y comunicación, como la tecnología facilita la comisión del hecho delictivo, el anonimato e identificación de los ciberdelincuentes, la tipificación de estas conductas es difícil y poco específica por la constate evolución de nuevos ciberdelitos, el desconocimiento del riesgo por parte de la sociedad, la extraterritorialidad, los pocos recursos humanos y herramientas para la investigación (Rayón y Gómez, 2014).

Barrera (2019) sostiene que los procedimientos de investigación en el mundo virtual tienen una alta probabilidad de fracaso, por los elementos que representan realizar este tipo de investigación, debido al delicado tratamiento que deben tener las evidencias digitales, acompañado por la negligencia, desconocimiento o falta de experiencia de la víctima o del agente con información relevante, perdiéndose de manera irreversible. Con herramientas utilizadas por los delincuentes para hacer compleja la investigación, impidiendo la navegación y rastreo en la red.

La individualización e identificación de los autores de estafas por medios electrónicos por parte de la fiscalía es una labor compleja, debido a que utilizan identificación falsa, igualmente las empresas que venden un producto o servicio. Debido a la experiencia de los ciberestafadores los delitos quedan impunes por la capacidad de pasar desapercibidos, por eso muchas víctimas prefieren no denunciar, debido a que la justicia no realiza los procedimientos que corresponden a las investigaciones, para que estas lleguen a juicio. Otro problema es la tipificación tardía de esta conducta dentro los códigos, por consiguiente, realizar tratados con todos los países del mundo para cumplir sus investigaciones. (Cortez, Haydee y Lagos, 2020).

El delito de estafa se considera de resultado material, por consiguiente, exige un resultado lesivo, en este tipo de delito, por la disminución cuantificable del patrimonio económico por causa del engaño. Este fenómeno delictivo debe contar con una atribución del patrimonio económico en un sentido amplio, comprendiendo la suma de las relaciones jurídico-patrimoniales, perteneciendo todo bien de naturaleza económica con apariencia jurídica, sin importar su reconocimiento jurídico (Balmaceda, 2016).

Las estafas a través de medios cibernéticos o informáticos forman parte del ciberdelito, y está a su vez es considerada una categoría dentro del estudio de la criminología por el avance indiscutible de las tecnologías, donde el ciudadano tiene acceso con un ordenador o por un teléfono móvil a través de un plan de internet o tarifa de datos, siendo un medio instaurado en la sociedad, donde no es negativo por sí solo, depende del uso que le dé (González, 2014).

Gómez (2020) explica que las estafas se pueden clasificar en tres tipos, la primera es ordinaria donde se le atribuye los elementos del engaño para producir un desplazamiento económico, también considerada la estafa vulgar, la segunda es la estafa tecnológica si bien es lo mismo que la ordinaria, esta añade el uso de un

medio tecnológico o internet, y por último la estafa informática donde el principal elemento es manipular máquinas para sustraer una disposición económica.

Las estafas de internet o en línea pueden ocurrir de diferentes maneras, a través de correos electrónicos, el denominado phishing, redes sociales, mensajes en el móvil, llamadas falsas, scareware, entre otros, con el objetivo del apoderamiento de tarjetas de créditos, credenciales de inicio de sesión y contraseñas, terminando con el robo de identidad (Norton LifeLock Inc., 2021).

Balmaceda (2011) en la revista de derecho y ciencias penales sobre el tema de las estafas Informáticas en el derecho europeo continental, la denominación de estafa informática aparece exclusivamente a las defraudaciones patrimoniales causada por medios informáticos, con la mayoría de doctrinas europeas estiman que la estafa informática y la tradicional deberían estudiarse estrechamente.

Según Marazzo (2020), la evolución de la tecnología no solo es una ventaja para la comodidad en diversas actividades, sino que también ha traído una adaptación de las estafas tradicionales, convirtiéndose en estafas informáticas, utilizando mecanismos informáticos para engañar a las personas y obtener un beneficio económico.

A nivel internacional organizaciones como la ONU, y en el conteniente europeo como la Unión Europea y el consejo de Europa, hacen un llamado sobre la actualización de los procedimientos de investigaciones relacionadas a los medios digitales. Para esto las organizaciones sugieren a los países tomar medidas en la adaptación de las Leyes Procesales Penales en la investigación de este nuevo escenario (López, 2016).

La Oficina de las Naciones Unidas contra la Droga y el Delito (2013, citado por Godoy, 2020) expuso que

> **En 2011 al menos 2.300 millones de personas, equivalente a más de un tercio de la población total del mundo, tuvo acceso a Internet. Más del 60% de todos los usuarios están en los países en desarrollo y el 45 % de todos los usuarios de Internet tienen menos de 25 años. Se estima que para 2017 las suscripciones a la banda ancha móvil llegarán, aproximadamente, al 70 % de la población mundial. Para 2020 el número de dispositivos interconectados por la red ("Internet de las cosas") será seis veces mayor al número de personas, lo que transformará la concepción actual de Internet. En el mundo hiperconectado del futuro será difícil no imaginar un "delito informático", o quizás ningún delito, que no implique pruebas electrónicas relacionadas con la conectividad del protocolo Internet.** (p.116)

Más de 2850 millones de usuarios activos al mes, Facebook, la red social más usada del mundo, no escapa de las estafas en sus diversas modalidades en línea. ESET Latinoamérica, compañía en detección de amenazas informáticas, describe las estafas comunes en Facebook, como el phishing, los préstamos falsos, cuentas clonadas, estafas a través de Live, concursos, criptomonedas, falsas donaciones, anuncios fraudulentos, estafas de compras y falsas advertencias para hacerse pasar por Facebook en los correos y mensajes (Guzmán, 2021).

Con un aumento exponencial en los delitos informáticos, Argentina reporto un incremento de un 80 %, donde Julieta Zanazzi, especialista en Derecho de la ciberseguridad y entorno digital, expuso que las estafas informáticas se pueden dar en dos grandes grupos, a través de Skimming, referente a la clonación de tarjetas, y el grupo relacionado a estafas a través de correos electrónicos, mensajes de texto o llamadas telefónicas (Marazzo, 2020).

En Argentina, los estafadores implementan una modalidad de engaño, que consiste en comunicarse de manera telefónica con las víctimas, donde se hacen pasar por gestores del ANSES, que es la administración del seguro social en argentina, sacando información, secuestrando la cuenta y sacar un préstamo a nombre de las personas estafadas, llegando a transferir 80 000 pesos argentinos que equivale a 812.33 dólares americanos (Harán, 2020a).

Datos de la sección Internet Crime Complaint Center (IC3) del Buró Federal de Investigación (FBI) de los Estados Unidos, informó que en el 2016 se recibió un total 12 005 reclamos por estafas de correos falsos para transferencias bancarias de los departamentos de finanzas de grupos corporativos, esta acción denominado Business Email Compromise, con pérdidas de 360 millones de dólares. También ese mismo año se dieron estafas de soporte técnico, donde ciberestafadores engañaban a las personas para obtener rescate de la información y cuentas bancarias, esta modalidad recibió 10 850 reclamos, generando pérdidas de 7,8 millones de dólares. En casos de extorsión por el hurto de datos se establecieron la cifra de 17 146 casos, perdiendo más de 15 millones dólares (Pagnotta, 2017).

El FBI de los Estados Unidos registra una cifra de 791 790 delitos cibernéticos en 2020, responsables de 4 200 millones dólares perdidos, aumentando con un 69 % a comparación del 2019, y con respecto a las estafas informáticas el Centro de Denuncias de Delitos por Internet del FBI recibió 28 500 denuncias (Owaida, 2021).

Con un incremento de 200 % de delitos informáticos durante el confinamiento de países por el COVID-19, según estimaciones la Comisión de Seguridad Ciudadana del Parlamento Latinoamericano, por eso Juan Pais, Presidente del Parlatino, sugiere un proyecto de ley sobre el cibercrimen (Rodríguez, 2020).

Harán (2020b) plantea que los delincuentes aprovechan las compras en líneas para realizar estafas con el uso de plataformas sociales, phishing, falsificación de plataformas de comercio electrónico entre otras estafas, aumentando hasta un 70 % de aumento en España según los datos de la Guardia Civil, mientras que en argentina era de un 50 % asegura la Unidad Especializada en Ciberdelincuencia.

El 22 octubre de 2013 la Asamblea Nacional de Panamá aprueba el convenio sobre la ciberdelincuencia, hecho en Budapest en 2001, siendo el segundo país

latinoamericano, con el objetivo de salvaguardar y proteger a la sociedad panameña de la ciberdelincuencia, cooperación entre los Estados y sector privado, esto para contrarrestar el ciberdelito de manera rápida y eficaz (Giménez, 2014).

Fratti (2016) expresa que el Código Penal de Panamá no incluye a los delitos que se realicen por medios electrónicos, y con la implementación del Convenio de Budapest en Panamá debería buscar reformas del Código Penal. Tipificar nuevas tendencias delictivas como los hurtos digitales a bancos, acceso ilegal a sistemas informáticos, la instalación malware, spam, extorsión, fraudes, estafas, calumnia y difamación online, entre otros.

Según cifras del Ministerio Público en Panamá los delincuentes causan pérdidas por 20 mil dólares diarios, sin contar con las cifras negras, principalmente por las extorsiones en los centros penitenciarios del País, con un aumento del 344 % del 2016 al 2020. Con respecto al 2021, hasta mayo, se denunciaron 794 ciberdelitos, según el procurador encargado, con variantes en la sextorsión, la estafa, la pornografía infantil y el cibersecuestro. Señaló Juan Pinto, Ministro de Seguridad de Panamá, sobre la capacidad e inteligencia de los delincuentes para la manipulación de las herramientas tecnológicas en la comisión de delitos a través de medios digitales (Coriat, 2021).

Entre 2020 y 2021 hubo un incremento del 421 % en denuncias por delitos informáticos siendo la pandemia un factor generador de esta conducta. En el área metropolitana, las estafas a través de medios cibernéticos o informáticos corresponden al 68 % de las estafas totales, correspondiendo a 655 solo en el 2021 (Alvarado, 2021).

Producto del COVID-19, los ciberdelincuentes son beneficiarios de las limitaciones de movilidad e interacción social directa, por lo que las personas deben hacer uso de los medios tecnológicos y plataformas para cumplir con las actividades.

Panamá no escapa de este fenómeno delictivo, en palabras del mayor de la DIJ Bernardo Águila, sustenta que se han vuelto comunes los casos de estafa en compras online, por contacto a través de mensajería instantánea o web, por medio del engaño para obtener un beneficio económico (Jiménez, 2020).

En Panamá, Álvarez (2020), en el periódico Metro Libre, manifiesta que los delitos con el uso de tecnología incrementaron en un 130 % en la provincia de Panamá Oeste, registrando 2,888 casos vinculados al delito de estafas agravadas, por el uso de un medio informático, debido al incremento de las personas en la realización de teletrabajo, negocios electrónicos, el aumento de la banca en línea y el pago del bono solidario, creando elementos para la realización de este tipo de delito.

Una publicación en Twitter de la Policía Nacional de Panamá (2021) hace referencia sobre las cantidades de denuncias, situándose en más de mil denuncias en el último año con pérdidas económicas de aproximadamente 2.5 Millones de dólares por estafa, dando una perspectiva sobre el daño de esta conducta delictiva a nivel nacional.

En legislación panameña esta conducta se encuentra en el Código Penal (2007), y se refiere a una conducta agravada a las estafas, pues esta realiza daño al patrimonio económico con la utilización de medios informáticos. Con la inexistencia detallada en Panamá sobre esta conducta punible, y si bien contempla dentro del mismo documento de manera general señala el uso de los datos, la manipulación de aplicaciones, y redes, se puede favorecer a futuras conductas nuevas o no presentes en el territorio sobre las estafas informáticas, con el fin de dar un peso legal aun con la falta de especificación en los tipos de estafa con el uso de medios informáticos.

Uno de los últimos hechos registrado en la provincia de Coclé, por la Atención Primaria de Aguadulce, fue la Aprehensión de cinco estafadores en la modalidad

de llamadas telefónicas, un tipo de estafa a través de medios cibernéticos o informáticos, en donde se contactaban con a las víctimas para ofrecer un premio, y para hacerlo efectivo, debían depositar cierta cantidad de dinero, este ilícito está siendo investigado por 28 denuncias en la seccional de Aguadulce (Ruiz, 2021).

1.1.1 Problema de la investigación

¿Cuáles son los procedimientos que se realizan en la investigación judicial de las estafas a través de medios cibernéticos o informáticos en el corregimiento de Aguadulce?

1.2 Justificación

Ante lo expuesto en el planteamiento del problema, y considerando el aumento de este fenómeno delictivo en el año 2020, producto del COVID-19, y solo a medidos del 2021 esta cifra incrementa, por un mayor uso de las redes informáticas, debido a la obligación de las personas en el teletrabajo, el uso de la banca en línea, compras en redes sociales, y la educación de manera virtual, haciendo que la probabilidad de ser víctimas sea mayor, la investigación que se realiza es importante porque permitirá recabar información relevante sobre los procedimientos llevados a cabo, en Aguadulce, durante la investigación judicial de las estafas a través de medios cibernéticos e informáticos.

Este tipo de criminalidad tiene un aumento progresivo a través los años, surgiendo nuevas modalidades por parte de los ciberestafadores, afectando el patrimonio económico de los individuos, donde las autoridades estado o la localidad, debe implementar contramedidas para la solución de las estafas a través de medios cibernéticos o informáticos, implementando procedimientos de investigación innovadores, donde la interrelación del equipo de investigación judicial, llevados por el Ministerio Público auxiliado por la Dirección de Investigación Judicial y el

Instituto de Medicina Legal y Ciencias Forenses se complemente para solucionar este delito.

Además, señala las labores específicas y conocimientos de la DIJ y el IMELCF en la actuación de casos de esta modalidad de estafa, mostrando la capacidad que tienen nuestras autoridades de investigación, los recursos humanos, tecnológicos, procedimientos y estrategias.

Como una base de datos sobre el ciberdelito, las modalidades, victimarios y víctimas, para comprender el fenómeno delictivo digital general, y de forma específica sobre las estafas a través de medios cibernéticos o informáticos.

El equipo de investigación judicial puede verse abrumado por la gran cantidad de estafas agravadas por los medios cibernéticos o informáticos reportadas, cada vez mayor a medidas que pasan los años, donde estadísticas no muestran disminución. Donde las cifras negras están presentes, por la falta de confianza de parte de la población con la autoridad para la resolución de este tipo de delito, con la existencia de una hipercriminalización en nuevas modalidades de las estafas, y el equipo de investigación debe adaptarse a nuevos procedimientos.

Propiamente será una guía de consulta sobre los estafadores informáticos y las modalidades, con el fin facilitar la comprensión del hecho y poder realizar un proceso de investigación más rápido y sencillo, en la recolección de indicios y comprensión de los mismos, debido a que los procedimientos de investigación para el esclarecimiento de este tipo de estafa, requieren hacer uso de técnicas innovadoras, con el uso de dispositivos, aplicaciones y estrategias adaptables a la resolución de estos casos.

Es de importancia y urgencia que los investigadores conozcan sobre los procedimientos de investigación de estas estafas por el aumento progresivo, y no solo ellos, así mismo, la sociedad que se informe sobre esta conducta, como

puede suceder y los distintos tipos, para ser preventivos a la hora de utilizar un dispositivo informático, conociendo los riegos de ser estafados.

De igual manera, este documento se encuentra en información básica sobre los conceptos de procedimiento, los objetivos, principios y pasos generales en una investigación de un delito, para fortalecer los conocimientos posteriores y relacionarlos en investigaciones de delitos informáticos, específicamente en los de estafa a través de medios cibernéticos e informáticos.

El presente estudio beneficia de forma directa a las autoridades y cuerpos auxiliares de investigación criminal, aportando información sobre los procedimientos en los delitos de estafas a través de medios cibernéticos e informáticos. También se consideran beneficios académicos con la información suministrada, a estudiantes, principalmente a los de Investigación Criminal y Seguridad, y otras carreras afines.

Con beneficiarios indirectos de la comunidad, debido a que cualquier delito es dañino para la sociedad, y con respecto a las estas estafas, una conducta punible que está creciendo en los últimos años. La relación de los procedimientos de investigación de las estafas a través de medios cibernéticos e informáticos y la sociedad es realizar un trabajo eficaz en búsqueda de la descriminalización de esta conducta.

1.3 Hipótesis de la investigación

Ho. Los procedimientos utilizados por las autoridades correspondientes en las investigaciones judiciales de estafas a través de medios cibernéticos o informáticos en el corregimiento de Aguadulce son eficaces.

Hi. Los procedimientos utilizados por las autoridades correspondientes en las investigaciones judiciales de estafas a través de medios cibernéticos o informáticos en el corregimiento de Aguadulce no cumplen con las expectativas.

1.4 Objetivos de la investigación

1.4.1 Objetivo General:

Analizar los procedimientos utilizados para la investigación de las estafas a través de medios cibernéticos o informáticos en el corregimiento de Aguadulce.

1.4.2 Objetivos Específicos:

- Explicar sobre las estafas a través de medios cibernéticos o informáticos, y las distintas modalidades que se pueden presentar en el corregimiento Aguadulce.
- Mostrar la capacidad de las autoridades en la investigación judicial de E estafas a través de medios cibernéticos o informáticos en el corregimiento Aguadulce.
- Recolectar información sobre la situación actual de los procedimientos de investigación judicial en las estafas a través de medios cibernéticos o informáticos en el corregimiento de Aguadulce.

CAPÍTULO II

CAPÍTULO II MARCO TEÓRICO

2.1 Procedimientos de Investigación Judicial

Para establecer un concepto sobre procedimientos de investigación judicial debemos conocer el significado de las palabras que conforman esta noción, el primero es procedimientos, donde Torres (2019) lo define como un término de acción detallada sobre un proceso, mostrando la ejecución de los pasos que se deben realizar en una actividad, presentes de forma escrita o no en la organización; la investigación según la ASALE & RAE (2020) lo define como el efecto de investigar; y el concepto judicial donde el mismo autor lo define como la administración de justicia.

Con las nociones ya definidas de las palabras que conforman procedimientos de investigación judicial, se puede atribuir que esta terminología se puede encontrar de igual forma como investigación criminal.

Según González (2019)

> **La investigación criminal es un conjunto de conocimientos que se encargan de fijar la verdad de cómo sucedieron los hechos y determinar la responsabilidad de estos si están relacionados con el delito. Se establece a través de estrategias que papel jugó la víctima, el delincuente y como se llevó a cabo el delito; busca estratégicamente la manera de controlar y prevenir el delito, además a través de técnicas y conocimientos científicos se reconstruyen los hechos teniendo en cuenta durante qué tiempo, formas, y lugar, para determinar de manera más acertada como se dieron los hechos y la identificación de los posibles autores.** (p.30)

Básicamente lo que señala es sobre las técnicas, estrategias y el procedimiento que se debe emplear para lograr una investigación, donde el crimen es “cualquier acción que represente un daño social y no se halle tipificada como delito” (Morellas, 2013, p.45), en este sentido las investigaciones son dirigidas a mediar cualquier comportamiento que ocasione un peligro a las personas, sin importar su denominación dentro de las leyes.

Conociendo sobre lo que es Investigación Criminal, se establece la relación en el uso de las herramientas, técnicas y estrategias contra un delito, el mismo “se produce cuando la acción no causa un daño social, pero aparece tipificada como delito” (Morellas, 2013, p.45), es decir que no todos los crímenes son delitos, donde dependerá de las normas establecidas dentro de la sociedad.

De acuerdo a lo expuesto previamente, una definición acertada sobre la investigación judicial es:

> **La investigación judicial y criminalista es definida como una disciplina autónoma que tiene como propósito auxiliar a la justicia mediante el análisis y la aplicación de técnicas, métodos y procedimientos sustentados por diversas ciencias, que le permiten obtener información y procesarla a fin de identificar el “modus operendi” y el autor de un delito.** (García, 2015 citado por Pesantes, Valarezo y Vilela, 2019, p. 445)

Con lo planteado anteriormente, se puede definir como el conjunto ordenado de pasos para llevar a cabo la investigación de una conducta considerada delictiva dentro del código penal de un país, pues la misma tiene un carácter dentro de la administración de justicia, y se adaptará a las características del fenómeno delictivo, para establecer las estrategias adecuadas a la situación y recursos disponibles.

2.1.1 Objetivos de la investigación criminal

En el lugar de los hechos, las investigaciones judiciales deben tener objetivos planteados de manera general para ser proactivos. El equipo de investigación debe tener presente aspectos básicos de comprensión general sobre cómo llegar a cumplir su labor.

Para Lago (2017) los objetivos son:

> a) **Investigar los hechos consignados en denuncia o querella.**
> b) **Determinar si se ha cometido o no un hecho punible tipificado en las normas penales.**
> c) **Identificar, con base en los análisis de resultados técnico-científicos y de las diligencias judiciales, a los responsables del hecho criminal.**
> d) **Junto con la autoridad judicial competente, propender a la captura del delincuente(s) o persona(s) comprometida(s) en el delito.**
> e) **Aportar pruebas y participar en todas las etapas del proceso penal.**
> f) **Recuperar los bienes sustraídos y ocupar aquellos en que haya una flagrante comisión de un hecho punible o como resultado del desarrollo investigativo que adelanta en compañía de la autoridad judicial competente respectiva.** (p.14)

Generalmente el autor determina los objetivos básicos que debe tener toda investigación criminal, los mismo aplicarían en la investigación judicial, por los explicado previamente en el punto anterior.

Los equipos de investigación de delitos deben aspirar a implementar estos objetivos en la resolución de hechos delictivos, esto quiere decir, que tanto los investigadores, como el equipo de criminalística, los criminólogos, entre otras autoridades están involucradas; por lo cual el personal investigador debe establecer objetivos específicos dependiendo del tipo de hecho que se investiga, considerando las características de modo, tiempo y lugar.

2.1.2 Principios de la investigación Judicial y criminalística

Para lograr las investigaciones se deben tener constancia de los principios fundamentales y básicos en una investigación de un delito, todo investigador judicial debe conocer e implementar en los casos, donde por sus nociones generales se adaptan a cada tipo de delito. Pesantes, Valarezo y Vilela, (2019) sostiene que estos principios fundamentales de la investigación judicial y criminalística son:

- Principio de Uso: todo hecho delictivo necesita un instrumento o material para comisión del mismo. En un caso de estafa a través de medios informáticos o cibernéticos sería el dispositivo, como un ordenador o teléfono móvil.

- Principio de producción: es el empleo del instrumento o material para cometer la conducta delictiva. Siguiendo con el ejemplo previo, el ordenador para enviar correos de bancos engañosos o el teléfono móvil para realizar llamadas con premios falsos.

- Principio de intercambio: Es el inevitable intercambio entre los elementos y participantes del hecho delictivo. Se pueden atribuir a la ip, los mensajes y el mensaje enviado del Ordenador y el teléfono móvil.

- Principio de correspondencia: es la vinculación del autor con el hecho delictivo. Sería en este caso de agravante de estafa, la comprobación que el autor está vinculado con el teléfono móvil o con el ordenador, su número y cuentas de acceso o correo.

- Principio de certeza: verificación mediante pruebas de laboratorios la relación de un elemento estaba en el lugar de los hechos o tiene relación el hecho ilícito. Prosiguiendo con el ejemplo de esta modalidad de estafa, las pruebas de laboratorios son analizadas por expertos en ciberdelitos o estafas, con el estudio del ordenador o el celular para determinar su relación con el hecho.

- Principio de reconstrucción: es la representación de los hechos sucedidos, mediante los elementos estudiados para crear un escenario más parecido a lo sucedido. Con una representación de cómo realizaron este tipo de estafa, reconstruyendo los pasos que realizaron los autores para cometer el ilícito.

- Principio de probabilidad: en conjunto con el principio de reconstrucción, establecen la teoría más probable. Determinar los procedimientos o pasos ejecutados por el autor de las estafas mediante el ordenador o teléfono móvil.

Estos principios son fundamentales para establecer normas generales aplicadas en los procedimientos de investigación judiciales, ajustándose a las características del delito a resolver, orientando al equipo de investigación sobre estrategias a lograr, para cumplir los objetivos de investigación.

Cada uno de ellos aporta de manera significativa una regla sobre los pasos de una investigación y la interacción de los elementos de un hecho delictivo, dependiendo entre sí, es decir, que cada principio requiere que el equipo de investigación haga uso del principio anterior para seguir con el próximo, porque el siguiente requiere de la información para cumplirlo.

2.1.3 Fases generales de la investigación judicial

Las fases de investigación son las que permiten determinar el hecho delictivo, compuesta de pasos específicos, debido a que el sistema de justicia de un país en general necesita comprobar la existencia de un delito con una investigación previa, como es el caso de Panamá, que existe la investigación previa para vincular a los indiciados con el posible hecho delictivo, para posteriormente iniciar la fase de investigación.

Rayón y Gómez (2014) expone las fases generales de investigación:

- **Fase previa, para comprender qué ha pasado, en qué ha consistido el delito y cómo se ha podido perpetrar;**
- **Fase de investigación propiamente dicha, para esclarecer quién es el posible responsable y si ha perpetrado efectivamente alguna acción punible;**
- **Fase incriminatoria, en la que se obtienen y aseguran las pruebas del delito para la posterior fase de enjuiciamiento.** (p.220)

2.1.4 Pasos de la Investigación Judicial

Es necesario seguir una serie de pasos en la investigación de un hecho delictivo, con el fin de esclarecer lo sucedido, el equipo de investigación establece un orden lógico para iniciar la investigación, como debe seguir y culminar.

Según el Instituto de Investigaciones Jurídicas de la UNAM (2013) los pasos metodológicos que permiten investigaciones eficaces son:

1. La observación: se inicia con el análisis de las características de los hechos, con el fin de obtener información necesaria para ser comprobada por técnicas de investigación científicas.

2. Planteamiento del problema: cuestionarse sobre los hechos a través de preguntas que lo llevarán a reconocer el problema. Estas preguntas son ¿qué?, ¿cómo?, ¿cuándo?, ¿quién? y ¿por qué? sobre este hecho.

3. Formulación de hipótesis: respondiendo a las preguntas del planteamiento del problema se establecen diversas hipótesis sobre el delito, con un grado de probabilidad por los elementos aportados en el análisis.

4. Experimentación: con el estudio a través de técnicas científicas se procede a la reconstrucción del hecho, para comprobar todas es la hipótesis y comprender el delito.

5. La teoría: esta etapa es el resultado final de la investigación, afirmando lo sucedido y las características que implicaron el hecho delictivo.

La efectividad de estos pasos en la resolución de un hecho delictivo, dependerá de las autoridades encargadas de la investigación, así mismo, de los recursos disponibles en el procedimiento. Debe ser una tarea en conjunto con profesionales

idóneos en diferentes campos, para ofrecer diversas perspectivas sobre el mismo hecho, con una conclusión acorde a los recursos invertidos y el compromiso de parte del equipo de investigación.

2.1.5 Técnicas en los procedimientos de Investigación Judicial

Estas técnicas son el conjunto de métodos y herramientas de carácter científico en la investigación judicial, con ventajas en la resolución de los casos, aportando información en la realización de las hipótesis y teorías, en la recolección de indicios, estudio científico de las evidencias, y el análisis general de un hecho delictivo, con la determinación exacta del modo, tiempo y lugar según los elementos obtenidos, estudiando todas las características circunstanciales del lugar de los hechos.

Es una necesidad imperiosa para el equipo de investigación conocer técnica que ayuden a la resolución de los hechos punibles, presentando diversas disciplinas, trabajando bajo un mismo objetivo, aportando recursos y datos en búsqueda de la justicia.

Las herramientas o métodos más utilizados en los procedimientos de investigación de un delito, según Leal (2011) son:

- Huellas dactilares: la dactiloscopia, con el estudio de las crestas papilares de ambas manos, puestos en una superficie, donde por sus diversos puntos característicos particulares en cada individuo. Con ventajas de aparecer en cualquier superficie en las escenas de un delito, y con el avance de la tecnología ha permitido el uso de sistemas de identificación capaces de reconocer las huellas en segundos.

- ADN: sustancia química más importante actualmente para la identificación, por la individualización del código genético en cada uno de las personas, ha

permitido dar un 99 % en el material encontrado en el lugar de los hechos. Puede ser encontrado en los restos biológicos como las fibras, huesos, y fluidos corporales, entre otros.

- Descripción física del individuo y los rasgos morfológicos o antropomorfos: son las características físicas de un individuo utilizadas para la identificación criminal, como la altura, peso, tipo de cuerpo o complexión, rasgos faciales o cualquier otro aspecto que permita su identificación, como los tatuajes, cicatrices y operación quirúrgicas.

- Identificación de las piezas dentales y mordidas: se hace presente la identificación de las piezas dentales y mordidas del agresor a través de la odontología forense, comprobada ser muy útil, debido a que una mordida al igual que las huellas dactilares, encontrar dos iguales, es de dos y medio billones a una de probabilidades.

- Acústica forense: Con la identificación de las voces recuperadas de las grabaciones de llamadas, notas de voz, acento usado, palabras utilizadas y por la respiración de los individuos, a través de un diagrama visual a través presentados por los expertos para comparación.

- Interrogatorio: Utilizada por las unidades de la policía judicial, donde el equipo de investigación debe tener la experticia, ingenio y la capacidad en hacer hablar a los indiciados, imputados y detenidos. Esta técnica tiene la finalidad de averiguar todos los elementos implicados de un delito, así como información relevante para el caso y cotejar la relación entre los elementos probatorios.

- Reconocimiento por fotografías: también conocida como rueda de reconocimiento, se identifica por medio de fotos las personas indiciadas e imputadas de un delito.

- Grafología: identificación de la caligrafía y cuerpo de la escritura, donde los expertos forenses toman características como la letra, palabras expresadas, circunstancias personales. Esta se ve apoyada por la Documentología Forense, que es el estudio de la tinta y el papel en los documentos, así como la falsificación y copias de los mismos.

- Inspección ocular y reconstrucción de los hechos: se puede formar hipótesis de lo que sucedió en el lugar de los hechos al observar las escenas, por las características del entorno, como las salidas, entradas, ubicación e indicios vistos de manera general, posteriormente con el estudio de todos los elementos recolectados e información, se realiza la representación de una verdad científica y técnica de lo que sucedió.

- Las cámaras de grabación: a través de la identificación de los sospechoso y fuente de información inédita, por su representación de indicios de manera gráfica, y con el uso de las cámaras de video vigilancia en diversos lugares, permite que los investigadores puedan obtener imágenes de actos relacionados de un delito.

- Estudio de armas de fuego y proyectiles: mediante la Balística Forense, se identifican los restos, huellas y dibujos de los proyectiles, así como los dibujos dejados en las balas en su salida y golpe trasero por el percusor, con elementos recolectados la policía judicial o científica identifica el arma y el proyectil.

Con todas estas técnicas aplicadas a los procedimientos de investigación judicial, la probabilidad de conocer la verdad sobre un hecho ilícito es mayor, agilizando la función de los investigadores, y con un pensamiento de siempre encontrar nuevos indicios para concluir exitosamente su labor.

Las técnicas deben ser utilizadas por el especialista idóneo a su campo, con un trabajo en conjunto de las disciplinas forenses y métodos de investigación criminal relacionadas con las características del hecho punible.

2.1.6 Procedimientos de Investigaciones Judiciales en Panamá

En Panamá, los procedimientos de investigaciones judiciales son realizadas por el Ministerio Público (MP), auxiliados por la Dirección de Investigación Judicial (DIJ) y el Instituto de Medicina Legal y Ciencias Forenses (IMELCF), con la labor de intervenir en el procedimiento de Investigación Judicial, aportando las técnicas y herramientas de carácter científico.

La Constitución de la República de Panamá en el título VII, capítulo 2° sobre el Ministerio Público, establece textualmente lo siguiente:

> **1. Defender los intereses del Estado o del Municipio.**
> **2. Promover el cumplimiento o ejecución de las Leyes, sentencias judiciales y disposiciones administrativas.**
> **3. Vigilar la conducta oficial de los funcionarios públicos y cuidar que todos desempeñen cumplidamente sus deberes.**
> **4. Perseguir los delitos y contravenciones de disposiciones constitucionales o legales.**
> **5. Servir de consejeros jurídicos a los funcionarios administrativos. 6. Ejercer las demás funciones que determine la Ley.** (Art.220)

El Ministerio Público de Panamá, por lo previamente expuesto, tiene diversas funciones relacionadas con la justicia, al ser un organismo autónomo, y no depender de los poderes del Estado, puede ser un mediador y defender, cuidando los intereses de la sociedad panameña.

Se pueden resaltar en sus funciones, la persecución de los delitos y contravenciones de deposición constitucional o legales, es decir, realizar los procedimientos de investigación judicial de los delitos expresados por la constitución y las leyes, como el Código Penal de la República de Panamá, El Código Procesal Penal de la República de Panamá, y demás leyes impuestas por los poderes del Estado.

Uno de los auxiliares del MP es el IMELCF, aportando las ciencias y laboratorios forenses en la investigación judicial, Según la Resolución N° DG-173-19 (2019) que actualiza el Directorio de Servicios Periciales del Instituto de Medicina Legal y Ciencias Forenses están divididos por secciones, y a su vez compuestas por diversas unidades, las cuales son:

Cuadro N°1. Servicios Periciales del Instituto de Medicina Legal y Ciencias Forenses

Sección	Unidades
Sección de Clínica Médico Legal.	Unidad de consulta externa. Unidad de Odontología Forense.
Sección de Malapraxis Médica.	Unidad de Malapraxis Médica.
Sección de Salud Mental Forense.	Unidad de Psiquiatría Forense. Unidad de Psicología Forense.
Sección de Patología Forense.	Unidad de patología forense.
Sección de Criminalística de campo.	Criminalística de Campo. Unidad de revelado Lofoscópico. Unidad Forense de Explosiones e Incendios.
Sección de Identificación Criminal y Civil.	Identificación Criminal y Civil. Unidad de Trazología Forense.
Sección de Balística Forense.	Balística Forense
Sección de Fotografía Forense y Video Forense.	Fotografía Forense. Unidad de Extracción, Fijación y Análisis de Video.
Sección de Documentología Forense.	Documentología Forense.
Sección de Planimetría Forense.	Planimetría Forense.
Sección de Accidentología Forense.	Accidentología Forense. Unidad Mecánica Automotriz Forense.

Sección de Morfología Facial.	Morfología facial. Unidad de señas y signos.
Sección de Informática Forense.	Informática Forense.
Laboratorio de Química Forense.	Química Forense.
Laboratorio de Biología Forense.	Biología Forense.
Laboratorio de Análisis Biomolecular.	Análisis Biomolecular. Unidad de base de datos de ADN.
Laboratorio de Bioquímica Clínica.	Bioquímica Clínica.
Laboratorio de sustancias controladas.	Sustancias controladas.
Laboratorio de Toxicología Forense.	Toxicología Forense.

Fuente: Resolución N° DG-173-19, 2019.

Compuesto de multidisciplinarias disciplinas, técnicas y métodos para auxiliar la resolución de los delitos, donde cada ciencia forense se adapta a las particularidades que rodean todo el esquema del lugar de los hechos para comprobar los indicios, y ser para convertidos en evidencias que utilizara el equipo de investigación.

Otro auxiliar del Ministerio Público es la DIJ, con funciones diferentes al IMELCF en los casos de investigación Judicial, esto con el fin de estar presente en todas las circunstancias y elementos atribuidos a un delito.

La Ley 69 (2007) en el capítulo I, sobre la Dirección de Investigación Judicial, en su artículo 2 describen sus funciones, en relación con los procedimientos de Investigación, está el de recibir informes de comisión de los delitos, práctica de investigaciones para el esclarecimiento de los delitos y vincular a los posibles autores, cuidar los distintos escenarios para preservar los indicios, asegurando las distintas materiales probatorios y elementos de pruebas, realizar entrevistas a los testigos, y los interrogatorios a los indiciados o imputados del hecho delictivo.

Estas entidades de la República de Panamá tienen un rol importante en la administración de justicia, aportando los elementos probatorios, respetando todas las normas y reglamentos adecuados en los procedimientos, cumpliendo con los objetivos, pasos y principios de una investigación criminal de un hecho delictivo.

2.1.7 Nuevas tecnologías en los procedimientos de Investigación Judicial

Estar a la vanguardia de las nuevas tecnologías en la investigación de los delitos, es una gran ventaja en la administración de justicia, por las nuevas estrategias, acompañada de los modernos equipos en la investigación que proporcionan mayor eficacia en la resolución de los hechos, sin que se pierda la calidad de los indicios o evidencias recolectadas. Esto supone que se pueden tomar números de indicio en el lugar de los hechos, tomando elementos probatorios anteriormente obviados, y las evidencias tratadas en los laboratorios serán de mayor provecho a la hora de presentarse como una prueba.

> **Conocer las técnicas y métodos empleados en la investigación criminal, se ha convertido en una necesidad imperiosa para no perderse en el mundo moderno en que nos encontramos dominado por el auge que tienen este tipo de disciplinas y materias en las culturas democráticas, donde la curiosidad por el mundo de lo prohibido y morboso, se ha disparado.** (Lean, 2011, p.22)

La idea planteada por el autor, amplía sobre la importancia de las nuevas tecnologías en los procedimientos de investigación, donde antes era impensable tener un dispositivo al alcance de la mano, como un celular inteligente, prácticamente mediante internet podemos obtener información existe sobre algún tema, estar en contacto con nuestros conocidos y hacer actividades importantes de nuestra vida cotidiana, como pagar una cuenta, hacer compras, estudiar y trabajar. Con tecnología de vanguardia, hacer frente a los diferentes hechos ilícitos cometidos con tecnologías de información y comunicación se hace que las evidencias digitales o cualquier medio probatorio de sea obtenido con mayor calidad, y libre de errores.

Al estar en constante actualización del procedimiento de investigación judicial es una gran ventaja, no solo para facilitar el trabajo de los investigadores, sino principalmente a los que reciben el servicio de la administración de justicia, la sociedad, por ella se da la existencia de los investigadores.

En este sentido, López (2016), dice

> **La utilización por la Policía de las modernas tecnologías constituye una herramienta de trabajo imprescindible para obtener las evidencias digitales del delito y contrarrestar los sofisticados medios de que se sirven los grupos criminales organizados, así como el carácter internacional de su actividad. La Policía tiene que contar con los medios necesarios toda vez que la eficacia de la actividad judicial probatoria se fundamenta, en última instancia, en la eficacia de la actuación policial previa.** (p.14)

Generalmente lo expresado por el autor, las autoridades deben estar a la vanguardia de las nuevas tecnologías para enfrentar los hechos delictivos, donde las evidencias digitales son la clave para añadir nuevos elementos probatorios, contrarrestando los actos delictivos cometidos por los grupos delictivos. Algo que destaca en las nuevas tecnologías, es rapidez en la que se puede compartir información, con esto dar una presencia internacional a las bases de datos de los delincuentes y modalidades de delitos.

2.2 Ciberdelitos

Si bien la investigación tiene el objetivo de conocer la naturaleza de las estafas a través de medios cibernéticos e informáticos, los delitos informáticos, mejor conocidos como ciberdelitos, como categoría de delitos realizados con tecnologías de información y comunicación, entonces se considera este tipo de estafa dentro de los tipos de los ciberdelitos, por eso para mayor comprensión del tema explicaremos aspectos relevantes de esta conducta.

Los hechos delictivos están presentes en todo el mundo, y desde tiempos antiguos, en constante evolución y adaptación de parte de los delincuentes, aprovechando la falta de conocimiento de las personas, siendo víctimas de

diferentes modalidades y más si son conductas realizados a través de medios informáticos, donde el desconocimiento de los ciberdelitos en la era digital, hacen una víctima participante o inocente de un hecho.

Loredo y Ramírez (2013) escribió

> **Los antecedentes de los delitos informáticos van a la par del desarrollo de las tecnologías de la información. Con el desarrollo de la tecnología, la sociedad se ha visto en un panorama de avance y desarrollo en todas sus áreas; por desgracia, la delincuencia también se ha beneficiado de esto.** (p.45).

Según Subijana (2008, citado por Pons, 2017), los ciberdelitos tienen cuatro características que permiten el aumento de los ciberdelincuentes, como la fácil comisión, los pocos recursos requeridos, las lagunas legales, por la falta de especificación en las jurisprudencias de un Estado y aunque esté dentro de las leyes, estos delitos pueden ser cometidos sin estar de forma física en el país que se realiza el hecho.

Estas características hacen que el ciberdelincuente esté seguro y confiado de seguir realizando este comportamiento, donde el anonimato, la complejidad en las investigaciones y la falta de leyes específicas incrementan exponencialmente estos delitos.

Los ciberdelitos son cometidos a través de las tecnologías, con la inexistencia de una criminalidad específica, sobre diversas conductas, afectando la información y comunicación, por esto en la actualidad, la ciberseguridad debe estar presente en nuestra sociedad. El Estado debe tener ámbito penal específico para estas estafas, y no establecer agravantes dentro de otra conducta delictiva (Fernández y Martínez, 2020).

Básicamente el autor sugiere aplicar la prevención del ciberdelito mediante la ciberseguridad, como herramienta clave en la protección de la información y comunicación, esto implementado por la sociedad, es decir, que cada individuo

debe ser precavido en el uso de la tecnología y el Estado debe crear políticas para el uso seguro de los sistemas informáticos.

Establecer lo que se puede definir como ciberdelitos dependerá de las legislaciones de cada país, pero existen definiciones generales sobre lo que es esta conducta.

Según Fernández y Martínez (2020)

> **El término ciberdelito permite englobar todos los delitos cometidos a través de las nuevas tecnologías, y aunque no es fácil determinar las conductas que se incluyen en los mismos, hemos de tener en cuenta a efectos legales la utilización de sistemas y datos informáticos como el objeto material del delito, el instrumento para su comisión y el simple soporte de la información.** (p.27)

Esto incluye todas las tecnologías de información y comunicación, como son los ordenadores, celulares, tabletas, etc., con el uso del internet y las páginas en líneas, para Jewkes y Yar (2013, citado por Barrio, 2018) es, “cualquier ilícito penal por medio de (o asistencia de) sistemas informáticos, redes digitales o internet y demás TIC” (p.38), siendo un concepto fácil de entender.

Todas estas tecnologías de información hacen posible un mundo globalizado, con solo acceso a una red de internet poder realizar diversas actividades. Algunos individuos ven la posibilidad de realizar un ciberdelito, aprovechándose de las características de estas conductas para su beneficio.

González (2011) señala

> **Las posibilidades de globalización e internacionalización que tales tecnologías ofrecen, junto con las indudables ventajas que supone el llevar a cabo actuaciones que pueden producir sus efectos incluso en otro continente, convierte a estas categorías criminógenas en aún más peligrosas y efectivas de lo que hasta el momento venían siéndolo, y en cierta manera generan un clima de miedo, inseguridad e impunidad, unas veces real y otras distorsionado.** (p.90)

Esta sensación de miedo, puede surgir por la falta de conocimientos de los ciberdelitos, y los modus operandi de los ciberdelincuentes, también la

inseguridad e impunidad, surgido de los vacíos legales, y la poca confianza de la sociedad para mediar este tipo de delitos.

2.2.1 Ciberespacio

Cabe considerar que en los ciberdelitos, se debe conocer el lugar o espacio donde se desarrollan este tipo de conductas delictivas, algo básico para toda investigación judicial, debido a que la escena del hecho es en medio para obtener elementos probatorios, conocer las características del entorno, modifica los procedimientos de investigación para ser adecuados a la situación.

Curtis (2011, citado por Pons, 2017), describe ciberespacio

> **Podemos describir al espacio cibernético, o ciberespacio, como un dominio artificial construido por el hombre, diferenciado de los otros cuatros dominios de guerra (tierra, aire, mar y espacio); aunque se haya formalizado recientemente, el ciberespacio puede afectar a las actividades en los otros dominios y viceversa. Además, el ciberespacio no está aislado sino profundamente vinculado y apoyado por medios físicos, por ejemplo, las redes eléctricas.** (p.81)

Por supuesto que este entorno muy relevante para las tecnologías de comunicación e información, donde la sociedad depende de su funcionamiento para realizar nuevas actividades relacionadas con la comunicación interpersonal, trabajos, sistemas automatizados, y todo lo relacionado a las tecnologías de comunicación e información.

Según Gasperin (2015, citado por Martínez, Leyva, Felix, et al.), el ciberespacio es el contenido dentro del internet, conformado por multiusuarios que hacen uso del de la red sin tener algún conocimiento, denominados cibernautas. Un espacio para realizar actividades digitales, como los mensajes, la web, contenido multimedia en red, y todo contenido digital, como una suma de información electrónicamente disponible, con interacción en tiempo real o posterior.

Desde ese punto de vista, el ciberespacio es muy importante en esta era, permitido a el desarrollo de las actividades de forma globalizada, cabe destacar que no todo es positivo, debido a que también es el nuevo lugar de los hechos en los delitos, en este sentido González (2011) expresa que este nuevo medio conduce a la evolución de riesgos, vinculados a la información compartida, los datos almacenados y los sistemas, que deben ser mediados protegidos por estrategias de ciberseguridad.

Los procedimientos de la investigación judicial deben adaptarse al nuevo entorno, con un equipo especializado con conocimiento sobre la ciberdelincuencia, y el nuevo lugar de los hechos, así mismo, tener herramientas tecnológicas que permitan la interacción con el ciberespacio.

La Universidad Internacional de Valencia (2021) argumenta que la protección de los datos, software y hardware es importante, cada vez se producen más ciberdelitos, subiendo las probabilidades de ser propensos a ser víctimas de diversas amenazas, como el phishing, Ransomware, entre otras. Por eso la ciberseguridad es importante, donde por medio de estrategias se logra la seguridad de la información y de los dispositivos tecnológicos, y se previenen las ciberamenazas.

Visto de esta forma, la ciberseguridad ofrece un sistema de navegación seguro en el ciberespacio, con estrategias de protección encaminadas a un espacio seguro en las actividades con tecnologías de información y comunicación.

2.2.2 Tipos de ciberdelitos

Con gran variedad en los métodos y herramientas tecnológicas de información y comunicación, la cantidad de tipos de ciberdelitos va incrementando, debido a que los delincuentes se aprovechen de las vulnerabilidades de este espacio, tomando mayor ventaja a comparación delitos realizados de forma presencial por el

victimario. Cabe destacar que algunos delitos informáticos por las características que presentan pueden ser realizados con mayores frecuencias, debido a los recursos disponibles de los ciberdelincuentes.

Los autores Loredo y Ramírez (2013) dicen que los ciberdelitos más comunes son:

- **Ataques contra sistemas y datos informáticos.**
- **Usurpación de la identidad.**
- **Distribución de imágenes de agresiones sexuales contra menores.**
- **Estafas a través de Internet.**
- **Intrusión en servicios financieros en línea.**
- **Difusión de virus.**
- **Botnets (redes de equipos infectados controlados por usuarios remotos).**
- **Phishing (adquisición fraudulenta de información personal confidencial).** (p.45)

Los ataques contra sistemas y datos informáticos, también denominado ciberataque, es el conjunto de acciones ofensivas contra los sistemas de información, como las bases de datos, servidores, redes, entre otros, con el fin de provocar daño a un individuo, grupo de personas, organización, empresa. Entre estas conductas podemos encontrar el robo de datos a usuarios o empresa, secuestro de datos, virus informáticos, descargas automáticos y ataques a la web (Bello, 2020).

Las ventajas que tiene realizar estas conductas a través del ciberespacio, aumentan la cantidad exponencialmente, y más si los objetivos de alto perfil, donde se puede obtener un gran beneficio por los ciberdelincuentes.

La usurpación de la identidad o también conocida como la suplantación de la identidad es utilizar información de otra persona para hacerse pasar por ella, esta se da de dos formas, mediante el acceso de la cuenta del usuario, obtenidos a través de otros ciberdelitos, también se da la usurpación a través de la creación de un perfil falso con información personal del individuo suplantado (Grupo Ático34, 2019).

Crear una identidad en redes, es una tarea sencilla, donde con la información básica de un individuo se puede hacer pasar por esa persona, pues los registros en redes sociales, solo necesitan un nombre, apellido y un correo para crear una cuenta.

La distribución de imágenes de agresiones sexuales contra menores a través de medios digitales, por el avance tecnológicos de las cámaras digitales y teléfono móviles inteligentes, y por la globalización del internet ha generado un crecimiento exponencial en el tráfico de imágenes y videos de abusos sexuales a niños y jóvenes (Álvarez, 2020)

Sin duda los delitos relacionados a las agresiones sexuales son graves para la sociedad, y más para las personas víctimas, ahora la implementación de las tecnologías de información y comunicación en estas modalidades, hace que el delito sea aún peor, dañando la integridad de los individuos por compartir esas imágenes.

La estafa informática es realizar conductas como la manipulación y engaño para obtención de un bien patrimonial, esto mediante la utilización de la tecnología capaz de modificar y alterar los sistemas informáticos, o así mismo con el uso de los dispositivos de comunicación para obtención de un bien económico de un tercero.

Mediante Intrusión en servicios financieros en línea o fraudes financieros, son el conjunto ciberdelitos relacionados con la usurpación de la identidad de un banco, correos de bancos falsos de instituciones financieras, robo de los datos de las tarjetas de créditos y débitos, entre otros relacionados a los servicios financieros en línea (Juárez, 2017).

Las pérdidas o la alteración del patrimonio económico es uno de los problemas en la economía, y por la modernización de los servicios financieros para ofrecer mayor calidad, rapidez y comodidad a los usuarios, el uso de tecnologías de información y comunicación se hace necesaria, pero estos pueden tener consecuencias como los ciberdelitos vinculados a la intrusión en estos servicios.

Los virus informáticos son aquellos que alteran las estructuras del hardware y software de los dispositivos informáticos, como los ordenadores o servidores, alterando los archivos y dañando datos. Los tipos de virus según su modo de acción son los de sobrescribir, parásitos, virus acompañante, vínculos infectados y virus destructivos, donde cualquier individuo en el ciberespacio puede ser afectado (Blog de CEUPE, 2020).

En resumidas cuentas, es uno de los ciberdelitos más conocidos, debido a que se pueden presentar en un dispositivo en diversas formas, impidiendo las actividades normales del sistema y dependiendo del virus, pueden hasta dañar completamente el dispositivo.

Ahora bien, uno de los ciberdelitos más peligrosos es el botnes, o también denominado ataque zombis, a través de herramientas los delincuentes inhabilitan equipos de terceros para fines ilícitos.

El botnes es la acción donde el ciberdelincuente, a través de diversos dispositivos secuestrados por medio de virus informáticos, para ser utilizados en el robo de información, inhabilitar el uso del dispositivo enviar spam y virus, siendo una de los ciberdelitos de mayor amenaza en internet (Avast Academy Team, 2016).

Cada uno de estas conductas son ciberdelitos comunes entre los países, donde cada técnica o metodología de empleo por parte de los ciberdelincuentes es diferente una con la otra, lo que supone un gran desafío en los procedimientos de investigación.

Las Autoridades encargadas en los ciberdelitos deben tener gran capacidad de adaptación para contrarrestar y prevenir, así mismo tener los recursos necesarios para realizar investigaciones, con especialistas, tecnología y un procedimiento general prestablecido en cada una de estas conductas.

2.2.3 Ciberdelincuentes

La diferencia entre los delitos tradicionales y los ciberdelincuentes, es el uso de los medios tecnológicos de información y comunicación en la comisión del hecho delictivo.

> **La delincuencia informática y los delitos relacionados con ella, suponen un tipo de criminalidad característica y especial (se diferencian la criminalidad informática, consistente en la realización de determinados delitos que sólo pueden materializarse a través de mecanismos informáticos o sobre los mismos programas y sistemas informáticos; y la criminalidad clásica relacionada con la informática, relativa a las guras delictivas tradicionalmente contenidas en los textos punitivos en los que la presencia de estas tecnologías no es sustancial a las mismas, sino instrumental).**(Fernández y Martínez, 2020, p.22)

Generalmente lo que exponen los autores, es sobre la evolución y adaptación de los delincuentes, antes los delitos relacionados con la informática, los dispositivos solo una herramientas, pero no se materializan en los mismos, es decir, delitos como la piratería de discos y casete, el robo y hurto de dispositivos informáticos, y todo relacionado con estos comportamientos, sin la materialización en el software, servidores o cualquier sistema informáticos, conductas actuales como el las estafas informáticas, hackers, ciberextorsión, entre otras, las que son ciberdelitos.

Arroyo, Gayoso y Hernández (2020) los que realizan este tipo de delitos, se les puede denominar de tres formas:

- Hackers de sombrero blanco o éticos: son los que se dedican a mejorar la seguridad de las empresas en donde son contratados, siguiendo código de

ética y guardando silencio sobre información de las vulnerabilidades de las páginas atacadas.

- Hackers de sombrero gris: ellos realizan los ciberataques para buscar la vulnerabilidad de las tecnologías de información y comunicación atacadas, así como compartir información confidencial.

- Hackers de sombrero negro: son los conocidos como los ciberdelincuentes, debido a que solo buscan su beneficio personal. Estos pueden ser los que son contratados por empresas para obtener información de otras organizaciones, y también los que realizan este comportamiento para obtener una ganancia directa.

Aunque los tres son profesionales en la realización de los ciberdelitos, solo uno es legal, y es el hacker de sombrero blanco, debido a que, si bien el hacker de sombrero gris realiza los ataques para verificar la seguridad, él no cuenta con los permisos para realízalos y el hacker de sombrero negro realiza estas conductas para obtener ganancias.

Con una ventaja en la comisión de estos hechos por las características que rodean los ciberdelitos, Centenos (2015, citado por Pons 2017) recalca que:

- Los ciberdelincuentes realizan estas conductas en cualquier parte del mundo, sin estar en el territorio en donde se realiza el ciberataque, lejos de las legislaciones de ese estado.

- El ciberacatante tiene confianza, debido a que no está físicamente expuesto a las circunstancias que presenta un delito tradicional, como los sistemas de seguridad físicas, como las barreras naturales o artificiales, el equipo de vigilancia conformado por equipos, como las cámaras, alarmas, también el

recurso humano en el lugar, como los guardias o vigilantes, los policías o guardaespaldas.

- Siente impunidad, por falta de cooperación internacional de parte de algunos países, sin normas específicas en las legislación o políticas encaminadas a la ciberseguridad.

- Aprovechando su anonimato en sus actuaciones ilícitas, donde los procedimientos de investigación para la identificación criminal son complicados.

- Cualquier individuo con acceso a un dispositivo tecnológico de información y comunicación, con conocimientos técnicos, una pequeña inversión puede realizar una conducta delictiva informática.
- Aprovechan la vulnerabilidad y la falta de seguridad informática individual para cometer el ilícito, también por el desconocimiento de la sociedad o del individuo sobre cómo protegerse.

Aprovechándose de las fortalezas en la realización de estas conductas, no es imposible considerar un aumento exponencial a través de los años, siendo el ciberespacio el nuevo lugar de investigación de los delitos.

2.2.4 Fases generales de la Investigación de los ciberdelitos

Los ciberdelitos son una nueva manera de cometer los delitos a través del uso de tecnologías de información y comunicación, por el lugar en donde se desarrolla, el ciberespacio, las fases de investigación tradicional pueden ser utilizadas, pero no serán eficaces, por eso existen fases para investigar los ciberdelitos.

Rayón y Gómez (2014) explican que la investigación de la delincuencia tecnológica o ciberdelincuencia tiene tres fases, si bien relacionadas con una

investigación tradicional, estas no tienen actividades diferentes para una investigación eficiente, y lograr objetivos diferentes y consecutivos, como:

Fase previa: se comprueba la existencia de un ciberdelito y establecer una teoría de cómo se perpetro, para esto se solicita información de los servidores correspondientes al tipo de delito, con el fin de comprobar los registros de los pasos que realizó el ciberdelincuente, mediante la utilización de logs, herramienta utilizada para conocer los detalles de operaciones realizadas en un sistema informático. Con esta herramienta se puede verificar mediante la IP del dispositivo, las páginas de internet visitadas, información del navegador, los servidores visitados y cualquier otra acción realizada en el equipo.

Dependiendo a las características del tipo de ciberdelito, algunos dispositivos informáticos no se pueden utilizar logs, por eso, por lo que se utiliza la recuperación de archivos borrados o restablecer el equipo a un punto anterior del sistema, este procedimiento se llama back-ups.

Fase de investigación propiamente dicha: una vez determinado el delito, se procede a determinar la manera en que se realizó el hecho. Posteriormente de realizar un análisis tecnológico para localizar e identificar el dispositivo, para conocer cómo se realizó, se debe comprobar la relación del dispositivo con el autor, algunos de los dispositivos encontrados pueden estar abandonados, llenos de virus o controlados remotamente, lo que complica la investigación.

Fase Incriminatoria: ya localizados e identificados, el equipo de investigación se dirige a la ubicación en donde se encuentra, posteriormente se recolectan los indicios relacionados con el hecho delictivo, se procede a realizar un análisis de todo el dispositivo, tanto el software y hardware. Este procedimiento se realiza manteniendo la integridad del dispositivo, para no modificar algún dato relevante en la investigación, si este procedimiento no es adecuado, puede generar problemas en fases posteriores del caso.

Todas estas fases expresadas por Rayón y Gómez, son generales en la investigación de un ciberdelito, por lo que en cada país puede haber mayor número de fases o son más específicas, dependiendo de las políticas criminales del estado, como las leyes, estrategias y personal especializado.

2.2.5 Víctimas de delitos informáticos

Los ciberdelincuentes aprovechan cualquier vulnerabilidad de los sistemas informáticos, base de datos o redes de información para obtener un beneficio propio. Observando cualquier de estos errores, utilizan las ventajas que le proporciona el ciberespacio y la falta de conocimiento de los individuos.

Neuman (1984, citado por Sevilla, 2012) expone que los tipos de víctimas son

> **VÍCTIMAS INDIVIDUALES. Distinguiendo entre aquellas que adoptan una actitud culposa o dolosa frente al proceso de victimización y las que carecen de tal actitud.**
> **VÍCTIMAS FAMILIARES. Entre las que se encuentran los niños y las mujeres maltratadas, así como todas aquellas víctimas de delito en el contexto familiar.**
> **VÍCTIMAS COLECTIVAS. En este perfil se encuadra a la comunidad como Nación con respecto a delitos como la rebelión y la sedición, y a la comunidad social frente al genocidio, los delitos económicos y el terrorismo, y a otros grupos sociales victimizados por el propio sistema penal (tortura, excesos en materia de prisión preventiva, etc.).**
> **VÍCTIMAS SOCIALES. Como pueden ser los minusválidos, ancianos o minorías étnicas victimizadas por el propio sistema social.** (p.25)

Los delitos informáticos no tienen distinción en los tipos de víctimas, debido a que existen diversas modalidades afectando de múltiples formas, afectando de forma individual, colectiva, familiar y social. Según Ellemberger y Wolfgang (1954, citador por Sevilla, 2012) la existencia de factores o elementos que hacen algunas personas sean víctimas de los delitos denominado como victimogénesis.

Existen divisos factores en los ciberdelitos que predisponen la existencia de muchas víctimas, debido a que muchas actividades anteriormente realizadas de forma presencial, ahora en la era digital, actividades como la educación, el trabajo,

la salud, el entretenimiento, la vida privada, en sí, todas las actividades que realiza la sociedad están influenciadas o utilizan las tecnologías de información y comunicación.

2.2.6 Marco legal panameño sobre los delitos informáticos

En Panamá los delitos relacionados al uso de las tecnologías de información y comunicación son mencionados brevemente en algunos artículos como un agravante o son mencionados de forma general, sin especificar qué conducta los individuos no deben realizar.

Delitos como las ciberestafas, la usurpación de identidad, los virus informáticos, el hurto informático, el botnets, la intrusión de servicios en línea o los ataque a sistemas están presentes de forma general en el Código Penal (2007), precisamente en el libro de delito, Capítulo XIII, “quien indebidamente ingrese o utilice una base de datos, red o sistema informático será sancionado con dos a cuatro años de prisión” (art. 289), haciendo referencia a los ataques informáticos, también expone en el mismo capítulo en otro artículo relacionado a los ciberdelitos.

> **Artículo 290 Quien indebidamente se apodere, copie, utilice o modifique los datos en tránsito o contenidos en una base de datos o sistema informático, o interfiera, intercepte, obstaculice o impida su transmisión será sancionado con dos a cuatro años de prisión.** (Código Penal, 2007, art. 290)

Ampliando las conductas en contra de los medios electrónicos, donde estas conductas están relacionadas a los ciberataques o también a la piratería informática. Al ser una interpretación general, puede adaptarse a diversas conductas realizadas por medios informáticos y de comunicación.

Panamá para adaptarse a estos nuevos delitos cometidos con medios informáticos, aprobó la ley 79 del 2013, relacionado con el Convenio de Budapest hecho en 2001, con el fin de luchar en contra de los ciberdelitos, donde se

muestran la explicación de algunos delitos, los procedimientos utilizados para obtener las pruebas digitales y la relación internacional de los países participantes de este convenio.

Según Pastorino (2017) el convenio de Budapest está conformado por 3 ejes esenciales para luchar en contra de los ciberdelitos, esto son:

- Primer eje en donde se muestran las definiciones de los delitos, presentando la tecnología como fin, tecnología como medio, características de los delitos y las infracciones a la propiedad intelectual.

- El segundo eje, explicando lo procedimientos para conservar las evidencias digitales, para evitar las pérdidas o alteración de las mismas.

- El tercer eje, es sobre la relación que deben tener a nivel internacional en la cooperación de investigaciones, no solo de delitos informáticos, también aplican los tradicionales.

Este convenio es una gran ventaja para Panamá en los procedimientos de investigación de los ciberdelitos, así como la implementación de nuevas herramientas y estrategias. La colaboración internacional a través de este convenio permitirá hacer un procedimiento efectivo en la resolución de los casos para determinar los autores.

- Procedimientos de Investigación en los delitos informáticos o ciberdelitos en Panamá

Los procedimientos de investigación de estos delitos al igual que otros, posteriormente de la denuncia o querella en la Fiscalía, se solicita la actuación por parte de la DIJ y la IMELCF para realizar las diligencias pertinentes. En estos casos por lo general actúa un equipo especializado, precisamente la sección de

Informática Forense, según la Resolución N° DG-173-19 (2019) se realizan las siguientes pericias:

a) El análisis e incautación de base de datos de ordenadores con un procedimiento incautación y recolección de equipos informáticos. Este procedimiento debe durar 7 días.
b) La incautación de datos de teléfonos y tarjetas SIM. Se recolecta información de contactos, mensajes, calendarios o cualquier elemento multimedia. Se debe cumplir en un periodo de 3 días.

c) Se dan procedimiento de incautación datos de almacenamiento digital y la recuperación de elementos borrados, para restablecer información pérdida, registro de programas instalados y multimedia. Tiene un periodo de realización de 7 días.

d) El rastreo e identificación de proveedores IP, donde con esto se puede obtener la dirección del proveedor del servicio de un dispositivo conectado a internet. Se realiza en 1 día esta pericia.

e) Analizar los sitios webs y correos electrónicos para observar el contenido existente, así como información de los propietarios o propietario. En 1 día de realiza este proceso.

f) Las redes sociales son analizadas para inspeccionar las características de una cuenta, y poder obtener información del propietario, como el número de conexiones, publicaciones e información general. Se realiza en 1 solo día esta diligencia.

g) Análisis de los equipos de fraude de tarjetas, con el fin de comprobar si este sistema informático funciona correctamente y no tiene ninguna modificación que altere su procedimiento requerido, con diligencias en la identificación de programas de tercero dañinos, extracción de imágenes, recolección de datos

de las citas magnéticas o también falsificación de las tarjetas. Su procedimiento tiene 15 días hábiles.

h) Se establece el análisis de información relacionada con la seguridad informática, a través de la inspección e identificación del acceso de usuarios, los sistemas y las actividades realizadas en el los equipos. La pericia se realiza tiene fecha límite de 1 mes hábil.

Todas estas pericias realizadas en Panamá tienen la finalidad de poder extraer elementos probatorios para vincular a un indiciado o atribuir la comisión de un hecho delictivo. De acuerdo con la fuente, todas estas diligencias tienen un plazo de culminación que dependerá de la dificultad del procedimiento, debido a que algunos solo son la observación para recolectar algún indicio y otros se debe realizar un conjunto de pasos para poder obtener información.

Con estos procedimientos realizados eficientemente, las investigaciones tienen un margen de probabilidad mayor de éxito, en determinar las características de un hecho en el ciberespacio o las modificaciones que utilizan los ciberdelincuentes para cometer el ilícito.

2.3 La estafa

Antes de conocer sobre las estafas informáticas, que es uno de los objetivos de la investigación, debemos considerar el término básico de esta conducta, con interpretaciones sobre la naturaleza de este fenómeno delictivo así mismo, se expondrá su historia, elementos, y cómo es considerada dentro de la legislación panameña.

Actualmente la estafa es aquella conducta en contra del patrimonio económico, esta no debe presentar violencia o amenazas de parte del sujeto activo, actuando de forma inteligente para engañar con medios fraudulentos a un individuo, y que

voluntariamente traspase un bien, también la misma debe tener un iter crimines secuencial en los elementos, debido que no se cumpliría como una estafa, sino una tentativa (Espinoza, 2018).

Westreicher (2020), define este delito como la obtención de ganancias por abuso de la confianza de un individuo mediante el engaño, donde el perpetrador tiene el consentimiento de la contraparte.

Con las definiciones de ambos autores se puede establecer un concepto general sobre a estafa, atribuyendo que es una conducta engañosa y con ánimo de obtener un bien patrimonial existente, donde intervienen un sujeto activo, en este caso el estafador, y uno pasivo, la víctima o víctimas del hecho.

La estafa afecta al patrimonio económico, debido a que afecta un bien de un individuo. Sánchez (2016) explica que patrimonio en el ambiento económico, son los derechos, obligaciones y bienes que un persona, grupo u organización tienen, estas pueden considerarse propios o heredadas

Se puede considerar que la estafa dentro de los delitos en contra del patrimonio económico, porque afectan un bien mueble o inmueble de un individuo, grupo u organización. Forman parte de estos delitos el robo, hurto, daños, apropiación indebida y usurpación.

2.3.1 Reseña histórica sobre la estafa

La estafa es un término moderno, debido a que no existía este comportamiento, o tampoco algún término con referencia a la estafa tradicional, pero sí conductas con todas las características para poder considerarlo a lo que conocemos actualmente como estafa tradicional, y posteriormente su forma nueva las estafas informáticas.

> **La estafa es un delito bastante moderno, ya que hasta bien entrado el siglo XIX lo que hoy entendemos como tal se castigaba a título de hurto o entre las falsedades, y sólo tardíamente se dio paso a una represión autónoma del engaño, en cuanto afectaba los derechos de otro, principalmente sus bienes.** (Hernández, 2003, citado por Leyton, 2014, p.124)

Este comportamiento existió desde la antigüedad, solo que se podía atribuir a un tipo de robo y hurto, dada en diferentes culturas que implementando normas para sancionar esta conducta.

Establecer el término de estafa similar a lo que conocemos en la mayoría de legislaciones actuales, pasó por diferentes modificaciones durante la historia, pero hubo culturas que destacaron en el desarrollo de esta conducta, iniciando con la cultura babilónica en el siglo XX a. C, con su implementación en el Código Hammurabi, el pueblo hindú en la Leyes de Manu, los persas, los musulmanes en el Corán, los romanos dentro de la conducta de falsedad, y por último los alemanes y franceses, implementando esta conducta de manera específica en las leyes (Gómez, 2014).

Las estafas fueron tema de discusión en todas estas culturas y pueblos, pero los romanos destacaron, denominando términos para sancionar conductas de falsedades, es decir, sancionaban conductas similares a con elementos de mentiras y manipulación, según Garrido (2012, citado por Leyton, 2014) “la estafa tendría su origen en el derecho romano, en el crimen falsi (Lex Cornelia de Falsis) que hacía referencia a las falsedades, pero con sentido más amplio al utilizado en el fraude” (p.124).

En evolución constante, donde en Roma no se estableció de forma definitiva las estafas, Quispe (2020) explica que “los romanos en un principio asignaron a la estafa como mal engaño o dolo malo (dolus malus); luego, como perteneciente al falsum; y, por último, cuando cedió a los reclamos del derecho privado y lo denominaron estelionato” (p.17). Si bien la estafa en Roma no era reconocida por ese nombre, se aplicaban sanciones por adquirir un bien patrimonial a través del

engaño. Terminologías de algunas conductas del pueblo romanas que a través de los años no han dejado de existir y tienen una definición dentro de las leyes hecho en la mayoría de países.

Yubero (s.f, citado por Espinoza, 2018) dice que el derecho romano consideraba a los delitos en perjuicio del patrimonio como estelionato, haciendo énfasis a la pluralidad de estos delitos, donde el Pretor, magistrado de la antigua Roma, determina las características del hecho y si este debía tener una pena.

Básicamente aun con la evolución de este término, su uso no era preciso, pues dependía de la autoridad encargada de los juicios para determinar si era tanto la apropiación indebida, la sustracción del uso o violación de la posesión mediante astucia o engaño, y que la autoridad encargada de solucionador el delito lo hacía bajo su criterio, determinando la pena que se debía aplicar.

Aplicar esta idea era innovador, pero no era el más óptimo para poder establecer bien las sanciones correspondientes, por ser muy general, y de poca especificación. Otra cultura que caracterizó la estafa, fue la alemana, con términos diferenciadores entre los delitos patrimoniales, anteriormente solo existía un todo en general sobre este tipo de delitos.

Según el autor Donna (2007, citado por Gómez, 2014) expone:

> **Posteriormente se fueron deslindando ciertos conceptos y es la ciencia alemana que la diferencia el fraude de la falsedad, ya que Feuerbach y Wachter definen la falsedad en el siglo XIX, y en 1820 y 1837 Cucumus aclara el concepto de fraude: manifestando que, objeto de fraude no era, según él, patrimonio en sentido económico, de la víctima, sino la facultad intelectiva de ella; para la falsedad no era necesaria la producción de daño. Por lo que, en este sentido se vislumbra el fundamento racional de incriminación en la lesión de un derecho social, la fe pública.** (p.6)

Y con esto diferenciando el concepto de estafa con los demás delitos de patrimonio económico, que en su momento el derecho alemán como la falsedad, y también diferenciándolo del hurto y el robo. Explicando qué comportamientos

engloban las estafas, así como las medidas de sanción que debe tener la autoridad a quienes realicen este comportamiento.

Con todos estos aportes en la historia, la denominación de este comportamiento fue de gran relevancia para ajustar a lo que conocemos en la mayoría de los países como estafa, si bien, cada país define sus delitos, los específica y define, los elementos para esta conducta son iguales o similares.

2.3.2 Elementos de las estafas

Son aquellas características que permiten distinguir la estafa de otros delitos, y más si son delitos relacionados con otros delitos que afectan el patrimonio económico, como el robo, hurto, usurpación, daños y la apropiación indebida. La estafa a través de la historia no estaba especificada, pero si existía con elementos, como el engaño que se utiliza para adquirir el bien mueble o inmueble de un tercero, pero en la actualidad se pueden definir criterios específicos para determinar esta conducta delictiva.

Según Leyton (2014), la estafa debe estar compuesta por cuatro elementos fundamentales, los cuales son el engaño, el error, la disposición patrimonial y perjuicio, para determinar este delito, relacionados entre sí para determinar objetivamente el autor del este delito:

El engaño puede describirse como las estrategias que usa el delincuente en la estafa para que la persona crea alguna situación o hecho. Según Antón (1958, citado por Balmaceda, 2011) el engaño es la “simulación o disimulación capaz de inducir a error a una o varias personas” (p.179), con este elemento que oculta la verdad de un hecho, los individuos que son objetivo de la estafa se vuelven víctimas posibles del hecho.

Siguiendo con el error, segundo elemento de la estafa, posteriormente después de caer en el engaño del delincuente, según Pérez y Gardey (2021), el concepto general del error es realizar alguna actividad de forma incorrecta o hacer algo equivocado.

Básicamente el error que cometen las víctimas en la estafa es caer en el engaño, esto por las estrategias de mentiras que ofrece el victimario, por lo llamativo de adquirir un bien o servicio que ofrecen, por una necesidad, o por el desconocimiento de las actividades realizadas por los estafadores.

Siguiendo con la disposición patrimonial, según Espinoza (2018), es la posesión o titularidad del bien del sujeto pasivo de la estafa, el mismo debe estar presente durante el elemento del engaño, y debe pasar del titular del bien al sujeto activo del delito, en este caso del estafador, la disposición patrimonial debe estar presente en esta conducta, si no se da la inexistencia de la estafa.

El autor expresa que, sin el patrimonio económico, de un bien mueble o inmueble, como el dinero, un auto, un terreno, o cualquier objeto de valor, en esta conducta, solo se produciría un engaño, y no un hecho ilícito como una estafa.

El último elemento, es el perjuicio patrimonial, refiriéndose al traslado del patrimonio económico del sujeto pasivo al sujeto activo completándose la estafa, Espinoza (2018), dice que posteriormente del desprendimiento patrimonial que está en el último elemento, el individuo resulta perjudicado y en tal caso no se realiza este traspaso, la estafa queda en tentativa.

Gutiérrez (1991, citado por Balmaceda, 2011) atribuye que

> **En definitiva, en la estafa es imprescindible un perjuicio económico, cuya determinación a nuestro entender únicamente podrá considerarse valorando al patrimonio en su conjunto –como universalidad de derecho–, antes y después del delito, atendiendo al valor económico de sus componentes y a la importancia económica que en el conjunto pueda tener el menoscabo –ya que de esta manera se evitan problemas a la hora de una "compensación".** (p.173-174)

Conocer el valor del patrimonio económico perdido a través de la estafa, ayudará en la resolución del delito, a la hora de determinar la sanción correspondiente y la restauración del bien sustraído por el engaño y manipulación.

También conocer el bien estafado ayudará a determinar los procedimientos en la fase de investigación, porque dependiendo al tipo de bien, ya sea mueble o inmueble el del equipo de investigación debe adaptarse.

Con estos cuatro elementos podemos determinar la existencia de un delito de estafa, donde debe cumplirse un orden de pasos, empezando con el engaño, siguiendo con el error, y por último la disposición patrimonial, y el perjuicio patrimonial.

Otros autores exponen que las estafas están compuestas por más elementos, siendo un proceso más específico en la determinación de esta conducta delictiva, según Castillo (2020) estos elementos son:

- El primer elemento es el engaño, representado a con alguna estrategia o artificio que usa el sujeto activo.
- El segundo es que la estrategia de engaño sea creíble y se adapte a los objetivos para incitar un traspaso patrimonial.
- El tercer elemento es el error, se da mediante la equivocación del sujeto pasivo por el desconocimiento del hecho.
- El cuarto elemento se da un desplazamiento patrimonial, donde el bien del sujeto pasivo es transferido al sujeto activo.
- El penúltimo elemento, es la existencia de un nexo casual, es decir, el perjuicio y dolo, es decir, que debe tener la intencionalidad de engañar.
- El último elemento que considera en la estafa, es el ánimo de lucro, defina como la intención del sujeto activo, en obtener el patrimonio económico.

Estos elementos en comparación con los anteriores presentados, están compuesto por más criterios para determinar la esta conducta delictiva, entre estos está el segundo, sobre las estrategias con la adaptabilidad del engaño hacia a los objetivos, también se añade el nexo casual, donde incluye el perjuicio y el dolo, a diferencia de la anterior clasificación, el dolo no estaba impuesto dentro de algún elemento, pero se entendía que la intencionalidad para obtener un bien de parte del victimario.

2.3.3 Tipos de estafas

Este delito puede tener diferente modalidad de parte de los estafadores, entre algunas de ellas pueden ser:

- Pedir dinero adelantado: el autor del delito se hace pasar por un vendedor, solicita un pago adelantado de un producto o servicio inexistente.
- Publicidad engañosa: los productos o servicios no tienen las características mencionan en publicidad del negocio o redes de comunicación.
- Falta de claridad en las condiciones de la transacción: se da cuando un vendedor luego de obtener un abono inicial o el pago del producto o servicio, solicita un extra al cliente para entregar lo acordado.
- Presentación de documentos falsos: con el uso de una documentación fraudulenta, como un carnet de identificación o certificado, solicitan un bien o servicio (Westreicher, 2020).

Estos son algunos tipos de estafas tradicionales que normalmente son los más comunes en la actualidad. Si bien cada modalidad presenta características unicas y un modo de acción para lograr su cometido, todas presentan los elementos necesarios para ser considerados como este delito.

2.3.4 Marco legal panameño sobre la estafa

En la República de Panamá, ese delito está tipificado en el libro segundo, referente a los delitos, situado en el Título VI, denominado Delitos contra el Patrimonio Económico, específicamente en Capítulo III, con el nombre de Estafa y otros Fraudes. Esto hace alusión cómo la República de Panamá se refiere a un hecho de estafa, así como las sanciones o penas por los diferentes agravantes de esta conducta delictiva. Textualmente el primer artículo referente la estafa expone:

> **Quien mediante engaño se procure o procure a un tercero un provecho ilícito en perjuicio de otro será sancionado con prisión de uno a cuatro años. La sanción se aumentará hasta un tercio cuando se cometa abusando de las relaciones personales o profesionales, o cuando se realice a través de un medio cibernético o informáticos.** (Código Penal, 2007, Art. 220)

El artículo anterior, hace referencia a al engaño, un elemento general en la estafa, previamente definido como las estrategias del sujeto activo, para hacer incurrir en un error al sujeto pasivo, y producir el hecho delictivo. Otra terminología presente es la de ilícito, refiriéndose a la ilegalidad de la conducta, está realizada en perjuicio, es decir, el traspaso del bien patrimonial.

El marco jurídico panameño está compuesto por las estafas simples y agravantes, con comportamientos específicos de una modalidad, así de noción general sobre tipos de estafa, con la función de cubrir cualquier modalidad de estafa que no esté especificado en el código penal.

Toda conducta tipificada en el Código Penal tiene una sanción simple, en el caso de la estafa es la privación de la libertada por 4 años, y esta aumentará si la conducta adquiere algunos criterios que la hacen más dañina. En el siguiente artículo señala el aumento de la pena simple previsto en el artículo 220, por los siguientes motivos.

> **La conducta prevista en el artículo anterior será sancionada con prisión de cinco a diez años en los siguientes casos:**
> **1. Si la lesión patrimonial excede de cien mil balboas (B/.100,000.00).**
> **2. Si la cometen apoderados, gerentes o administradores en el ejercicio de sus funciones.**
> **3. Si se comete en detrimento de la Administración Pública o de un establecimiento de beneficencia.**
> **4. Si se usurpa o utiliza la identidad de otra persona para obtener algún beneficio.** (Código Penal, 2007, art. 221**)**

Dentro del mismo capítulo se describen conductas específicas sobre algunos tipos de estafas, detallando el modo de actuar de los estafadores o requisitos que se tienen para determinar este delito.

El artículo 222 expone las estafas por los correos del seguro de forma ilícita, esto mediante la alteración intencional del bien asegurado, así como el daño propio, causado por lesiones, realizado por el receptor del beneficio del seguro, con un estimado de pena de prisión de 2 a 6 años; en el artículo 223 sobre las créditos obtenidos por medio de hipotecas de un bien inmueble, o de prenda de un buen mueble, donde los individuos mienten sobre las gravas, es decir, los impuesto para obtención del bien, también califican aquellos que utilicen un bien ajeno para obtener una hipoteca o prenda, esta modalidad tiene una pena de prisión de 4 a 6 años (Código Penal, 2007).

Generalmente estos dos artículos están relacionados con las estafas a instituciones financieras, como son las compañías de seguros, cooperativas y bancos.

El artículo 224 se refiere a la alteración, uso ilegal de los servicios y modificación dispositivos de medición para obtención de forma gratuita o con menor gastos, con pena de prisión de uno a dos años. El artículo 225 está relacionado con el artículo 224, sobre la modificación de dispositivos o equipo de medición, añadiendo actividades como la captación, interrupción, transmisión o retransmisión de forma ilícita de televisión o videos, con pena de prisión de 2 a 4

años, la misma tienen una opción de días multas si el daño no es mayor a 250 balboas (Código Penal, 2007).

Ambos artículos relacionados a estafas a los servicios, donde por el uso ilícito de los mismos, para no gastar dinero a través del engaño o estrategias fraudulentas a las empresas o los propietarios del servicio. El último artículo del capítulo III es el artículo 226, relacionado con las tecnologías de información y comunicación, posteriormente explicado en otro capítulo de la investigación.

2.3.5 La estafa y su diferencia con otros delitos contra el patrimonio económico

La estafa se encuentra vinculada con delitos contra el patrimonio económico, estos pueden variar dependiendo al país, tipificando sobre los elementos característicos de tal conducta. Los delitos contra el patrimonio se pueden traducir en la afectación de bienes de una persona como los muebles, inmuebles, tangibles, los títulos de valores y todo lo que tenga que ver sobre la posesión en sí misma.

Basándome en Código Penal de la República de Panamá los delitos contra el patrimonio económico son el robo, hurto, apropiación indebida, usurpación, daños y las estafas, señalando las distintas modalidades para determinar algunas de estas conductas, así como las penas.

Según el Código Penal (2007), tipifica el hurto como

> **Quien se apodere de una cosa mueble ajena será sancionado con prisión de uno a tres años o su equivalente en días-multa o arresto de fines de semana o trabajo comunitario. Igual sanción se le aplicará al copropietario, heredero o coheredero que se apodere de la cuota parte que no le corresponde, o a quien se apodere de los bienes de una herencia no aceptada.** (art. 213)

Algunas de las características que diferencia el hurto de la estafa, es sobre la falta de consentimiento de parte del dueño del bien, ya que en la estafa el bien es recibido con el consentimiento por el dueño.

El robo al igual que el hurto es el apoderamiento de un bien sin el consentimiento del dueño, según el Código Penal (2007) lo tipifica como, “Quien, mediante violencia o intimidación en la persona, se apodere de una cosa mueble ajena será sancionado con prisión de siete a doce años” (art. 218), tampoco se utiliza elementos de la estafa como el engaño.

Otros delitos diferentes en delitos contra patrimonio económico son la apropiación indebida, usurpación y los daños, el primero hace referencia a provecho de un bien o productos es esta, pero a diferencia de la estafa el bien es prestado a la víctima y no lo devuelve. El segundo, la usurpación, referente al empleo de violencia, engaño, amenazas, abuso de confianza o clandestinidad para obtener un bien inmueble, como un terreno o derechos, al igual que la estafa, esta puede presentar a través del engaño, pero con la diferencia que se utilizan de forma diferente, pues, en la usurpación puede ser usado el engaño para ocultar los límites de un bien inmueble, mientras la estafa usa el engaño como estrategia para lograr adaptarse a los objetivos; por último el daño, se puede establecer como la destrucción de un bien mueble e inmueble (Código penal, 2007, art. 227-229, 230)

Ya vistas las diferencias que tiene la estafa con otros delitos contra el patrimonio económico, se comprende que tiene características únicas a las demás conductas punibles de esta índole, con esto se debe establecer un procedimiento distinto a la hora de investigar para lograr los mejores resultados.

2.4 La estafa a través de medios cibernéticos o informáticos

La estafa está evolucionando a través de los años, con individuos que aprovechan las tecnologías de información y comunicación en la comisión de esta conducta a través de medios cibernéticos o informáticos, como se le tipifica en Panamá, también denominada en otras legislaciones o por otros autores como estafa informática, estafa en línea, ciberestafas o estafa tecnológica.

Formando parte de los ciberdelitos, y con un crecimiento exponencial en los últimos años, tomando fuerza en la globalización y la digitación de alguna actividad, como la educación, económica, en los aspectos sociales y la vida privada, entre otras.

Solo el uso de un dispositivo informático como es celular que es de uso cotidiano, solo con un mensaje puede causar un daño a un individuo, o con correos engañosos haciéndose pasar por empresas que ofrecen un servicio, llamativos, de bajos costos, donde individuos caen esta trampa dejándose llevar por los beneficios que tiene.

Las llamadas haciéndose pasar por personas, con argumentos engañosos obtienen información de personas para luego usar en próximas estafas. Con individuos que se dejan llevar por la emoción de haber ganado un premio, con la finalidad de obtener algún beneficio económico a cambio de poder recibir ese premio.

2.4.1 Concepto de estafa a través de medios cibernéticos o informáticos

Al igual que la estafa tradicional, existen diferentes concepciones sobre lo que podemos considerar como estafa a través de medios cibernético o informáticos, debido a que dependerá de las legislaciones.

Un concepto general sobre la ciberestafa, es un delito que tiene la finalidad de engañar a las personas, esto a través de la manipulación de informática u otras estrategias tecnológicas que permitan la obtención del bien económico, cabe destacar que también se pueden denominar como estafa por internet o estafa informática (Moreno, 2020).

En el Código Penal Panameño no hay un apartado sobre las ciberestafas que hable exclusivamente estas de los diferentes tipos, sino que son mencionadas como un agravado de los delitos de estafa tradicional, denominado a través de medios cibernéticos e informáticos. Lo más cercano a esta conducta es el artículo 226, y habla de la manipulación de las bases de datos, redes o sistemas informáticos.

Textualmente el Código Penal (2007) tipifica

> **Quien, para procurarse para sí o para un tercero un provecho ilícito, altere, modifique o manipule programas, bases de datos, redes o sistemas informáticos, en perjuicio de un tercero, será sancionado con cuatro a seis años de prisión.**
> **La sanción será de cinco a ocho años de prisión cuando el hecho sea cometido por la persona encargada o responsable de la base de datos, redes o sistema informático o por la persona autorizada para acceder a estos, o cuando el hecho lo cometió la persona valiéndose de información privilegiada.** (art. 226)

A grosso modo, este artículo es general, si bien establece la manipulación o modificaciones de programas, bases de datos, red o sistemas informáticos, no establecer conductas específicas sobre las estafas a través de medios cibernéticos o informáticos, La sanción establecida para estas conductas el artículo establece la mismas, sin importar el tipo de ciberestafas, dejando la decisión a los Jueces en la fase del juicio oral.

2.4.2 Tipos de estafa a través de medios cibernéticos o informáticos

Existen diferentes tipos de estafas a través de medios cibernéticos o informáticos donde cada uno tiene sus propias características por su modo de operar, para obtención del bien patrimonial. Conocer sobre los tipos de estafas informáticas que pueden existir, plantear procedimientos de investigación judicial adecuados.

Estas estafas se pueden establecer en dos grupos, el primero son aquellas ciberestafas en donde se utilizan las tecnologías de información y comunicación para realizar las estrategias de engaño dirigidos a terceros y el segundo grupo

conformado por la alteración de los sistemas informáticos con el engañando al equipo informático para obtener el bien patrimonial.

Entre las que utilizan las tecnologías de información y comunicación para realizar las estrategias de engaño dirigidos a terceros, está el phishing en sus distintos métodos y estafas mediante el envío de dinero, y el segundo grupo dirigido a las estafas al sistema de los cajeros automáticos o las maquinas POS.
Todos estos tipos de estafa se vuelve más común con los años, donde las personas que utilizan medios informáticos deben tener presente todas estas formas en que los ciberestafadores realizan estas conductas.

- Phishing

Esta modalidad es muy común cuando se habla de los tipos de estafas informáticas, mediante el uso de dispositivos de información y comunicación se contacta a un individuo, grupos de personas o institución para obtener datos mediante el engaño, McAfee (2021) afirma que el objetivo de esta conducta es robar información confidencial mediante el engaño de correos, mensajes, entre otros, para que el sujeto pasivo voluntariamente envíe o permita el acceso de la información.

Según Mariana (2015)

> **Actualmente la forma de phishing más utilizada es el envío masivo de correo electrónico con la finalidad de engañar a la víctima y que proporcione sus datos personales al "phisher". Aunque esta no es la única forma de phishing. En los últimos años esta actividad ha ido mejorando y cada vez es más difícil detectar un correo falso. Además, las técnicas han ido mejorando considerablemente y cada día hay más y mejores.** (p.10)

El empleo de diversas estrategias el denominado phisher, utiliza cada vez técnicas más complejas para autentificar la originalidad de un correo, mensaje, o llamadas telefónicas, etc., haciendo la labor de reconocer estas estafas más complejas.

Siendo una modalidad muy diversa de las estafas a través de medios cibernéticos e informáticos, se pueden dar diversos tipos de phishing, donde cada vez son más difíciles de detectar, pero con el mismo objetivo, obtener la información y el patrimonio económico de las personas.

Belcic (2021), establece que en esta modalidad se pueden tener diferentes estrategias, como:

- Phishing de engaño: es el más simple, donde el ciberestafador se hace pasar por una empresa o alguna persona para obtener confianza para realizar la estafa.

- Phishing personalizado: A diferencia de phishing realizados a gran escala, mediante el spam, este solo se centra en un solo objetivo, con el fin de adaptar la mejor estrategia para obtener la información y el bien patrimonial.

- Whaling: Hace referencia a los ataques de phishing a personas de gran relevancia política o económica.

- Fraude de CEO: Es usualmente utilizada después de haber realizado el whaling, donde con esa información los ciberestafadores engañan a los miembros de una empresa.

- Phishing por Dropbox y por Google Docs: Esta modalidad de phishing se centra en la falsificación de las nubes para que los usuarios inicien sesión y suban datos, para posteriormente obtener el bien patrimonial.

- Phishing de clonación: a través de la clonación de un correo electrónico, los estafadores envían a los contactos de ese correo un enlace malicioso.

- Manipulación de enlaces: mediante el envío de enlaces fraudulentos, donde se enmascaran en sitios populares para que el cibernauta acceda.

- Scripting entre sitios: es uno de los modos de phishing más complejo de los ciberestafadores, donde secuestran un sitio web oficial para obtener información de los visitantes.

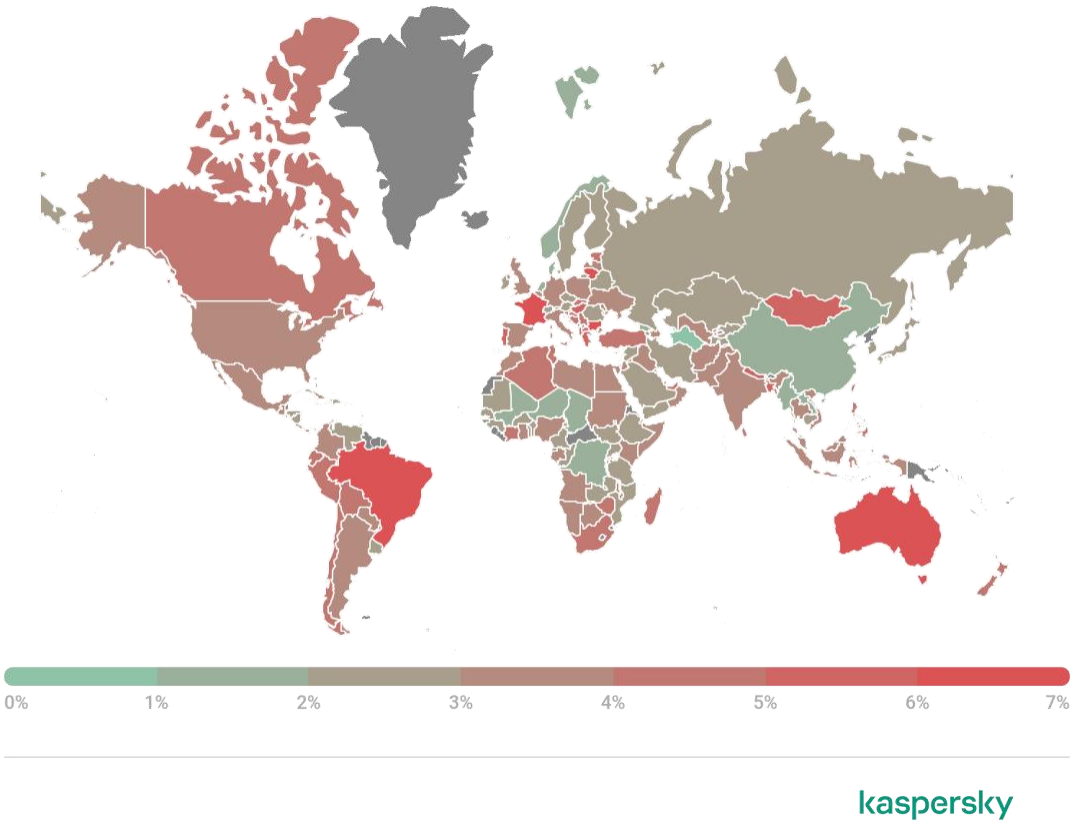
- Pharming: modalidad del phishing en la cual se realiza una copia o simulación de una web de un banco, con el fin de los usuarios accedan con su usuario y contraseña. Para que estos hagan uso del envío masivo de correo y el spam a los cibernautas.

Todas estas estrategias de los phisher utilizan los equipos informáticos para la realización de los procedimientos, donde cada uno tiene el fin de obtener información muy relevante, esta puede ser como los datos de una tarjeta de crédito o débito, documentos importantes, el usuario y contraseña de una cuenta de correo, o sitio web.

El phishing obtuvo un aumento del 70 % a nivel del mundo desde el inicio de la pandemia, en modalidades específicas como el phishing de clonación con 57 %, un 51 % en el whaling, 49 % en correos maliciosos, el robo de credenciales por correo con un 40 % y por mensajes SMS representado un 40 %, esto según la Phishing Insights, encuesta global realizada a 5 400 profesionales de tecnologías de información (Adam, 2021).

Existen diversos estudios estadísticos realizados cada año, o varias veces en un año sobre el phishing, mostrando la incidencia de esta actividad a nivel mundial o los principales objetivos de los ciberestafadores.

Gráfica N°1. Territorios de los ataques phishing, segundo trimestre de 2021.



Fuente: Kulikova y Shcherbakova, 2021.

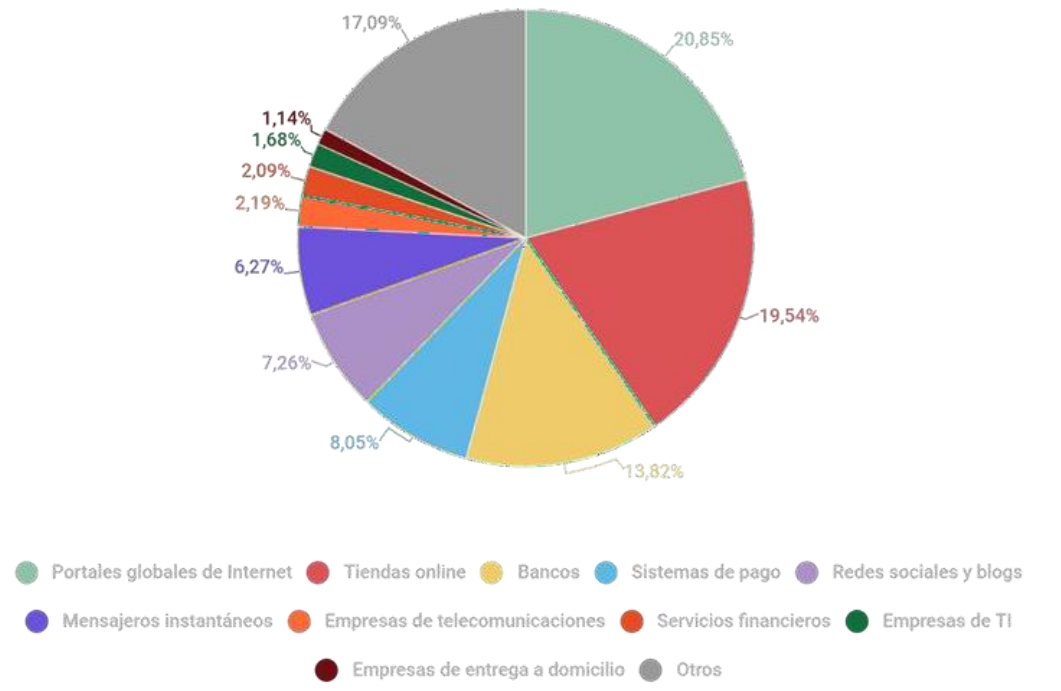
Esta gráfica muestra los países donde se presentan más activaciones de antiphishing en el segundo trimestre del año 2021. El estudio estadístico se dio con la recolección de información de las aplicaciones de seguridad informática que detectan el phishing como los antivirus, extensiones de navegador enfocado en la seguridad y privacidad, y el firewall o barrera de fuego.

Mostrando la cantidad a través de las tonalidades de color, siendo las tonalidades rojas con mayor cantidad de esta conducta y los verdes con menor cantidad. Los países con mayor cantidad en el segundo trimestre del 2021, lo encabeza Brasil, con un 6.67 %, siguiendo con 6.55 % con Israel, y Francia con un 6.46 %, donde los detectores antiphishing tuvieron más activaciones.

Cabe destacar que Panamá, aunque no esté presente en los primeros lugares, tiene una cifra del 4.15 % de las activaciones en los detectores de antiphishing, una cifra relevante si se compara con países con mayor población, como los Estados Unidos con un 3.82 % y México con un 3.27 %, o en el caso de países fronterizos, como Costa Rica con un 2,50 % y Colombia con un 3,87 %.

Considerar que los ciberestafadores que realizan el phishing atacan en diversas formas, utilizando los sistemas banca en línea, sitios webs, tiendas en líneas, mensajerías instantáneas, redes sociales, llamadas, entre otros.

Gráfica N°2. Distribución de organizaciones cuyos usuarios fueron atacados por phishers, segundo trimestre de 2021.



Fuente: Kulikova y Shcherbakova, 2021.

Los sitios webs en donde se reportaron más activaciones del antiphishing son los portales globales de internet con un 20,85 %, seguidos de las tiendas online con un 19,54 %, en tercer lugar, a través de otras páginas webs con un 17.09 %, en cuarto puesto la web de los bancos con un 13,82 %, siendo los cuatro sitios webs que utilizan los ciberestafadores para realizar sus métodos y las otras categorías de sitios webs no superan el 10 %.

Con esto observando que esta conducta no está definida en sí como un solo tipo de acción, sino que esta va buscando nuevas formas de causar daño al patrimonio económico a través del uso de los medios informáticos.

- Estafas mediante envío de dinero

Este tipo de ciberestafa es a través de aplicaciones o portales webs dedicados al envió de dinero, la estrategia de ciberestafadores ofrecen un producto o servicios en la web, como el marketing en línea, o también fingen una necesidad, esperando que algún usuario de internet quiera adquirir lo vendido o ayudar. Estas estafas los autores piden dinero adelantado, posteriormente de la transacción, bloquean al usuario o eliminan la cuenta.

Según el sitio web Ospina Abogados (2021) las víctimas de estas estafas son persuadidas, haciendo creer que van a recibir mucho más de lo que están pagando o ayudar a un individuo con problemas de salud. Estas modalidades se pueden dar por compras online, inversiones de criptomonedas, ofertas de trabajo, simulación del secuestro familiar y donaciones, entre otros.

La búsqueda de trabajo mediante la web se hace más común, antes de COVID-19, esta situación también existía esta práctica, por esto los ciberestafadores se hacen pasar por empleadores, ofreciendo propuesta de trabajos atractivas, como la de ser tu propio jefe. Con este engaño el estafador obtiene la información de

los usuarios, como la cuenta de bancos, número de tarjetas, correos, entre otros (Rhode, 2021).

Aprovechándose de la situación económica, ofrecer una propuesta de trabajo que puede solucionar la calidad de vida en lo económico, los individuos caen en el engaño y comenten el error de enviar información.

Las personas recuren al uso de tecnologías de información y para conocer a alguien, esto lo hacen mediante sitios dedicados a buscar parejas, o través de redes sociales, aquí los ciberestafadores ven la oportunidad de engañar a una persona.

Existen múltiples modalidades de engaño en las estafas de citas en línea o también conocidas como estafa romántica, entre estas modalidades el estafador engaña a la víctima para que le envíe dinero, regalos o información personal; otra modalidad es a través de la obtención de fotos o información personal, para pedir dinero posteriormente por eliminar esa información; la creación de perfiles falsos en sitios para conocer personas o redes para obtener dinero (Harán, 2019).

Siguiendo con estas estafas, también se da la modalidad de las estafas nigerianas, donde el ciberestafador se aprovecha de la ingenuidad y buena voluntad de terceros para requerir un tipo de apoyo por medio de un bien patrimonial.

> **Éste consiste en enviar mensajes electrónicos para pedir ayuda a los destinatarios, y de esta forma poder transferir importantes cantidades de dinero a terceros con la promesa de darles un porcentaje si aceptan esa operación a través de sus cuentas personales. Piden también que le transfieran a su nombre una pequeña cantidad de dinero para verificar los datos de la cuenta bancaria con la que se hará la transacción, o que simplemente les envíen los datos de la cuenta bancaria. Una vez que envíen el dinero, las víctimas no volverán a saber nunca más nada de esos estafadores.** (Sánchez, 2012, p.70-71)

Con la oportunidad de obtener un bien económico mucho mayor al que le está solicitando el estafador, esa estrategia para los cibernautas un modo incrementar sus bienes.

- Estafa a cajeros automáticos

Son estafas relacionas la obtención del dinero de un cajero a través de herramientas tecnológicas que permitan la obtención del bien patrimonial, esto de forma remota o directamente en el cajero automáticos. Entre estas conductas podemos destacar las siguientes:

El skimming es el uso de un dispositivo remoto y un hardware instalado en la parte superior del cajero automático, su función es transmitir la información de los datos de las tarjetas, posteriores crear un clon de la tarjeta y sacar el dinero (Asher, 2019).

El Jackpotting es un método de engañar al sistema de los cajeros a través de la modificación el sistema operativo, su modus de operar es hacerse pasar por técnicos de los cajeros para insertar al sistema un malware, posteriormente es controlar las operaciones, sacando 40 billetes cada 23 hasta vaciarlos, sus objetivos las instituciones responsables de dinero (Álvarez, 2018).

También a través de un móvil con tecnología NFC los delincuentes consiguen engañar al sistema, su estrategia es mover el móvil en cajeros con lectores de tarjetas de crédito sin contacto, debido a que esta tecnología NFC y con una aplicación diseñada para imitar a una tarjeta (Higuera, 2021).

Dotándose de diversas herramientas tecnologías para engañar a los dispositivos, así como el conocimiento técnico del funcionamiento de estos dispositivos los ciberestafadores aprovechan las vulnerabilidades de seguridad, principalmente de sistema operativo, modificando los valores de operar en los cajeros,

sobrescribiendo los datos y alterando el funcionamiento normal para obtener un beneficio económico.

2.4.3 Elementos de las estafas a través de medios cibernéticos o informáticos

- Manipulación informática y artificio semejante: es la utilización de las tecnologías de información y comunicación para modificar los datos o información existente en el ciberespacio sin el permiso de los propietarios. La finalidad de este elemento es obtener información para posteriormente usarla en los próximos pasos.

- Ánimo de lucro: es la intencionalidad por parte del ciberdelincuente de obtener un beneficio económico por medio de una ventaja.

- Engaño: elemento indispensable en las todas las estafas. En este caso sería crear estrategias mediante la manipulación informática, el fin de realizar un escenario lo más real posible para que el objetivo pueda ser persuadido.

- Producción del error: ya con las estrategias de engaño, se debe producir un error en el objetivo, esto puede ser por el desconocimiento de los usuarios, grupos o empresas.

- Transferencia patrimonial no consentida por el titular del mismo: es el traspaso del bien patrimonial de la víctima al delincuente.

- Nexo causal: para determinar que este delito es considerado como ciberestafa, debe haber una relación entre el engaño y el perjuicio, es decir, que el autor del hecho tiene la intencionalidad de hacerlo (Moreno, 2020).

Si bien el autor establece elementos, estos no cubren todo lo que establece las estafas través de medios cibernéticos o informáticos, ya que, existen diversos tipos de estafas, agrupados en dos grupos, los que utilizan las tecnologías de

comunicación e información para engañar a otros individuos en el ciberespacio y los que utilizan métodos para alterar los sistemas informáticos.

Por estas razones se puede establecer los elementos de estafas que utilizan las tecnologías de comunicación e información para engañar a otros individuos en el ciberespacio.

- El perjuicio o ánimo de lucro: antes de empezar a realizar el delito, el ciberestafadores selecciona los objetivos, con esto se da la intencionalidad de realizar esta conducta delictiva.

- Uso de la tecnología de información y comunicación: la existencia de estas estafas debe haber un dispositivo capaz de conectarse a al ciberespacio, y lograr modificar información de páginas web, servidores, correos o cualquier herramienta que necesiten los ciberestafadores.

- Engaño: a través de estrategias mostradas en el ciberespacio los ciberdelincuentes engañan los objetivos, con las modificaciones de los sistemas de información y comunicación.

- El error: se da cuando el objetivo es engañado y envía o escribe información a los ciberestafadores. Dependiendo a la modalidad de estas estafas puede ser complicado identificado conocer si eres una posible víctima.

- Transferencia: aquí puede pasar diversas maneras para obtención del bien, se da por medio de un chantaje por la información, o por el robo de datos que permitan al ciberestafador obtener el dinero por medio de tarjetas, banca en línea o cualquier sistema de transacción de dinero.

- Disposición patrimonial: debe haber un bien patrimonial para poder determinar la estafa informática, en general estas son por un bien mueble, como el dinero.

El grupo de estafas informáticas conformado por la alteración de los sistemas informáticos con el engañando al equipo informático para obtener el bien patrimonial, algunos de sus elementos son los mismos a los que utilizan los sistemas informáticos para el engaño un tercero. Manteniendo el ánimo de lucro, el uso de la tecnología y la disposición patrimonial, cambiando los elementos restantes.

El engaño es a los dispositivos de información y comunicación, como un cajero o las máquinas POS, esto a través de estrategias utilizadas por los ciberestafadores; el error sería de parte del dispositivo, como un cajero que reconozca una tarjeta de crédito falsa; y la transferencia sería por parte del dispositivo.

2.5 Delitos de estafas a través de medios cibernéticos o informáticos a nivel internacional.

Las estafas a través de medios cibernéticos o informáticos siempre están reflejadas por el uso de los medios de información, pero existen países que por sus características tienen una mayor probabilidad de que se comentan estafas informáticas debido al desconocimiento por parte de la sociedad, y las políticas criminales de un país.

Las leyes y normas son el resultado de la sociedad, debido a que las mismas se adaptan al pensamiento colectivo de un país, esto por las diversas tradiciones o cultura, y la influencia de la historia, pero en la medición de estas nuevas conductas, producto de la era digital, se deben establecer normas, leyes y convenios internacionales para poder realizar procedimientos de investigación eficaces.

Algunos de los países se pueden reflejar la estafa informática con un mayor índice, según Barreiro (2017) los 10 países más vulnerables al phishing son Brasil, Australia, Nueva Zelanda, China, Francia, Perú, Canadá, Qatar Y Georgia, utilizando sitios como Facebook, WhatsApp, páginas de bancos, sistemas de

pagos y tiendas online, esto en según el informe de Kaspersky, empresa rusa dedicada a la ciberseguridad.

Para solucionar esta problemática, algunos países crean acuerdos, y tratados, uno de lo más relevantes a nivel mundial es el Convenido de Budapest, con 65 estados miembros.

Según el documento Convenio Nº185 (2001), llamado convenio sobre la ciberdelincuencia o Budapest, este tiene los objetivos de buscar la cooperación de los países participantes, velar por una normativa penal común en los casos ciberdelitos, la manipulación de las pruebas digitales y la definición general de delitos informáticos. Uno de los artículos relacionados con las estafas a través de medios cibernético o informáticos, está en el Título 2, denominado delitos informáticos, en su artículo 8.

> **Las partes adoptarán las medidas legislativas u otro tipo que resulten necesarias para tipificar como delito en su derecho interno los actos deliberados e ilegítimos que causen perjuicio patrimonial a otro persona mediante: La introducción, alteración, borrado o supresión de datos informáticos; Cualquier interferencia en el funcionamiento de un sistema informático, con la intención, dolosa o delictiva, de obtener de forma ilegitima un beneficio económico para uno mismo o para otra persona** (Convenio Nº185, 2001, art.8).

El artículo hace mención sobre las medidas que deben adaptar los estados miembros participantes, así como los elementos que se deben considerar para este delito informático, en este caso la estafa informática, denominando en el convenio como fraude informático, pero el mismo hace referencia a la obtención del bien patrimonial de forma dolosa con la alteración o modificación del medio informático, haciendo referencia a los delitos de estafa cometidos a un sistema informático.

CAPÍTULO III

CAPÍTULO III: MARCO METODOLÓGICO

3.1 Diseño de investigación y tipo de estudio

La investigación tiene un enfoque o metodología mixta, donde se utiliza el análisis e interpretación sobre la información del delito de las estafas a través de medios cibernéticos o informáticos, los procedimientos investigativos judiciales y las distintas modalidades presentes en el Corregimiento de Aguadulce.

De acuerdo a Creswell (2010, citado por Arispe, Yangali y Guerrero, 2020) el enfoque mixto presenta las siguientes características:

> **1. Permite obtener una perspectiva más amplia y profunda del fenómeno de estudio.**
> **2. Ayuda a formular el planteamiento del problema con mayor claridad.**
> **3. Al tener múltiples observaciones se obtendrán más y variados datos. Por tanto, se pueden "explotar" mejor.**
> **4. Puede minimizar o neutralizar las desventajas de los enfoques cuantitativos y cualitativos.** (p.60)

Con un diseño no experimental, debido a que no se alteran las variables e inexistencias de un grupo de control, donde a través de técnicas de este tipo de enfoque, poder analizar los procedimientos de investigación sobre este fenómeno delictivo, según Arispe, Yangali y Guerrero (2020) "en estos diseños no se manipulan las variables, los fenómenos se observan de manera natural, para posteriormente analizarlos" (p.69).

- Tipo de estudio

El tipo de estudio, principalmente es descriptivo y explicativo, debido a las características estudiadas de los procedimientos de investigación judicial en los delitos de estafa a través de medios cibernéticos o informáticos, así como su naturaleza y su relación con la comunidad, también se aplica un estudio exploratorio, debido a la inexistencia de una investigación anterior sobre este fenómeno delictivo.

Según Pérez, Pérez y Seca (2020) el estudio o alcance descriptivos se utilizan en investigaciones con pocos datos, donde se realizan descripciones del objeto de estudio. El explicativo para analizar la situación o fenómeno, caracterizados por ideas y aportes que se establecen en las variables; y el exploratorio definido por ser temas muy poco estudiados o no investigados con anterioridad.

3.2 Población o Universo

Para el desarrollo de la investigación la población “se define como el conjunto de casos que tienen una serie de especificaciones en común y se encuentran en un espacio determinado” (Chaudhuri, 2018, citado por Arispe, Yangali y Guerrero, 2020, p.73).

En este estudio, se trabajó con dos grupos poblacionales. La primera población estuvo constituida por 16 funcionarios de instituciones auxiliares de investigación criminal, conformados por investigadores de la Seccional de Investigación Judicial del distrito de Aguadulce, y peritos de la Unidad de Informática forense de la Agencia del IMELCF en Los Santos, quienes atienden los casos ocurridos en las provincias de Coclé, Veraguas y la región de Azuero.

La segunda población, la conformaron residentes del corregimiento de Aguadulce, el cual, según el Instituto Nacional de Estadística y Censo (2013) en una proyección realizada a la cantidad de población en Panamá para el año 2020, tiene una población de 10 500 personas, de las cuales 7 644, se encuentran dentro de un rango entre 15 y 69 años de edad.

- Muestra

La muestra “se puede definir como ese subgrupo de casos de una población en el cual se recolectan los datos” (Arispe, Yangali y Guerrero, 2020, p.74). En la presenta investigación se eligieron las muestras de forma no probabilísticas, es

decir, “se seleccionan en base a la apreciación de los investigadores/as en función de determinados objetivos analíticos propios y particulares” (López y Fachelli, 2015, p.43), debido a la disponibilidad de la población a la hora de realizar las técnicas.

Atendiendo a la primera población, la muestra se conformó por un porcentaje de funcionarios de las instituciones auxiliares de investigación judicial descritas anteriormente. Los mismos, fueron elegidos de manera no probabilística por conveniencia del investigador, es decir, se aplicó la técnica de recolección de datos correspondientes en los días hábiles permitidos para la realización del estudio, teniendo en cuenta la disponibilidad de los funcionarios en el lugar.

De esta manera la muestra estuvo integrada por 11 funcionarios, con un porcentaje mayor al 45 %, equivalente a lo aceptado por regla de 3 en las investigaciones con población pequeña.

Tabla N°1. Tamaño de la muestra de funcionarios de investigación.

Funcionarios	Población	Muestra	Porcentaje
Investigadores de la SDIJ de Aguadulce.	13	8	62 %
Peritos de la Unidad de Informática Forense de Los Santos	3	3	100 %
Total	**16**	**11**	**69 %**

En cuanto a la segunda población, para la obtención de la muestra, constituida por una porción de los residentes del corregimiento de Aguadulce, se realizó la ecuación estadística para las proporciones poblacionales, para obtener una muestra correspondiente a un nivel de confianza aceptable del 95 % de confianza y 5 % de error, siendo de 366 habitantes.

Imagen N°1. Cálculo del tamaño de la muestra.

Fuente: Asesoría Económica & Marketing, 2021.

En principio esta segunda muestra estaría conformada por la cantidad resultante de la ecuación, sin embargo, el tiempo, la disponibilidad y la cantidad de muestras arrojadas por este instrumento, hacen difícil lograr los objetivos de este estudio.

Para contrarrestar estas limitaciones y obtener la perspectiva de la población en la investigación, se seleccionó un muestreo no probabilístico con muestra razonada, el cual, parafraseando a López y Fachelli (2015), es implementado por el juicio del investigador o por estudios anteriores, y es aplicable por limitaciones de tiempo y presupuesto, en donde se eligen a las muestras por características o casos específicos que se desea estudiar.

En la aplicación de este muestreo en la presente investigación se consideraron ciertas características para la elección de los participantes muestras, con el fin de obtener datos en igual condición, como el porcentaje equilibrado en el sexo, la

participación de todos los grupos de edades, que van desde los 15 a 69 años, los niveles de escolaridad, la disponibilidad y accesibilidad de los participantes por el COVID-19, así como determinar el tiempo de inicio y culminación para obtención de los datos. Cumpliendo con todas estas características se obtuvo la participación de 42 personas residentes del corregimiento de Aguadulce en la investigación.

3.3 Variables

Variable independiente: Procedimientos de Investigación Judicial.

Definición Conceptual (VI): “Las múltiples disciplinas del conocimiento humano para la consecución de sus objetivos y propósitos requiere la realización de un conjunto de actividades lógicas y secuenciales que facilitan la obtención de un objetivo” (Lago, 2017, p.16).

Definición operacional (VI): La resolución de los delitos de estafa a través de medios cibernéticos o informáticos pueden ser eficaces con el establecimiento de actividades ordenadas y lógicas, dando ventajas en el tiempo de reacción y organización de las autoridades competentes. Los procedimientos de Investigación criminal establecen una mayor seguridad a la población. Se medirán a través de los siguientes criterios:

- La capacidad para utilizar los Procedimientos de Investigación Judicial.
- Los conocimientos sobre los procedimientos para realizar de forma adecuada.
- El compromiso y responsabilidad de las investigaciones judiciales con los procedimientos correspondientes.

Variable dependiente: Estafas a través de medios cibernéticos o informáticos.

Definición Conceptual (VD):

> **Quien mediante engaño se procure o procure a un tercero un provecho ilícito en perjuicio de otro será sancionado con prisión de uno a cuatro años. La sanción se aumentará hasta un tercio cuando se cometa abusando de las relaciones personales o profesionales, o cuando se realice a través de un medio cibernético o informático.** (Código Penal, 2007, art. 220)

> **Quien, para procurarse para sí o para un tercero un provecho ilícito, altere, modifique o manipule programas, bases de datos, redes o sistemas informáticos, en perjuicio de un tercero, será sancionado con cuatro a seis años de prisión.** (Código Penal, 2007, art. 226**)**

Definición Operacional (VD): Las estafas a través de medios cibernéticos o informáticos es un delito difícil de medir por las características que representa esta conducta, por eso el conocimiento de la misma por parte de las autoridades beneficiará la investigación. La población es la directamente afectada, por consiguiente, exponer su perspectiva sobre las estafas informáticas. Los criterios para medir son:

- Conocimiento sobre las estafas a través de los medios cibernéticos o informáticos.
- Realidad y consecuencias de este fenómeno en la comunidad.
- Capacidad de contrarrestar este fenómeno delictivo.

3.4 Instrumento, técnica de recolección de datos y/o materiales

Los instrumentos utilizados son las entrevistas semiestructuradas y las encuestas cerradas, esto con el fin de poder dar respuestas a las hipótesis de la investigación y poder cumplir con los objetivos propuestos.

El primero es la técnica de la Entrevista de tipo semiestructurada, según Hernández y Fernández (2006, citado por Trejo, 2021) este tipo de entrevistas

“tiene la libertad de introducir preguntas adicionales para precisar conceptos u obtener mayor información sobre los temas deseados” (p.54).

La finalidad de entrevista semiestructurada en este estudio, es medir a detalle los conocimientos del personal encargado de los procedimientos de investigación judicial de las estafas a través de medios cibernéticos o informáticos en el Corregimiento de Aguadulce. Esta técnica utiliza como instrumento un cuestionario abierto de 6 preguntas para obtener la información relevante en a investigación.

La segunda técnica para obtener datos fue la encuesta cerrada, donde Kuechler (1998, citado por Trejos, 2020) establece que la encuesta es “la recolección de datos en el marco de una indagación para un estudio determinado mediante el uso de un cuestionario estandarizado administrado por entrevistadores especialmente entrenados o distribuida a una muestra seleccionada de encuestados” (p.56).

Esta técnica utilizó el instrumento del cuestionario, conformado por 3 preguntas generales, como la edad, sexo y nivel escolaridad, seguidos de 7 preguntas relacionadas a recabar datos sobre la perspectiva de la población del corregimiento de Aguadulce percibe la labor de los auxiliares de investigación en los procedimientos de estafas a través de medios cibernéticos o informáticos.

Las encuestas fueron realizadas por medio de la aplicación de Google Forms, implementando características para mejorar la obtención de los resultados, con la comprobación de los correos, la selección única y respuesta obligatoria en cada pregunta, así como el establecimiento de fecha de inicio el 4 de diciembre del 2021, y culminando el 6 de diciembre del 2021 en la aplicación de esta técnica.

3.5 Procedimiento

Etapa 1: Identificación del problema y elección del título. Inicialmente se procedió a realizar la búsqueda de un problema relacionado con la licenciatura, un tema actual o en potencial crecimiento, por consiguiente, concluyó en la elección del tema “Procedimientos de Investigación Judicial de Estafas a través de Medios Cibernéticos o Informáticos”, realizado en el corregimiento de Aguadulce en 2021 y 2022.

Etapa 2: Estructuración del primer capítulo y elaboración del segundo capítulo. Leídas las normas APA y el manual de trabajo de grado, se procedió a buscar bibliografía e infografía para fortalecer el planteamiento del problema, con sus antecedentes teóricos y la situación actual.

Etapa 3: Elaboración del capítulo II. Posteriormente de culminar la búsqueda de bibliografía e infografía, se confecciono la estructura el marco teórico de la investigación.

Etapa 4: Conceptualización de marco metodológico y selección de los instrumentos. Se establecieron las nociones y la selección de tipo de investigación, el enfoque, el tipo de estudio, la poblaciones y muestras, para seleccionar las técnicas de recolección de datos.

Etapa 4: Aplicación de las Herramientas. Posteriormente de ser validadas las herramientas de recolección de datos se implementó las técnicas para la recolección de datos.

Etapa 5: Tabulación y Análisis de resultados. Finalizando con el análisis de resultados, la conclusión, recomendaciones, limitaciones del estudio y anexos.

CAPÍTULO IV

CAPÍTULO IV: ANÁLISIS Y DISCUSIÓN DE LOS RESULTADOS

4.1 Resultados de las entrevistas aplicadas a investigadores y criminalista.

Cuadro N°2. Entrevista N°1

N°	Preguntas	Respuestas
1	¿Es frecuente la comisión del delito de estafas informáticas en el corregimiento de Aguadulce? ¿Qué modalidad es la más reportada?	Es frecuente, y más por el inicio de la pandemia ese delito se incrementó, por la necesidad de la sociedad en utilizar los medios tecnológicos, como las compras online, pagos de servicios, recibo y envíos de dinero. Con estas necesidades, los delincuentes aprovechan esta oportunidad. Si no me equivoco, las estafas más reportadas es el secuestro virtual por medio de llamadas telefónicas, donde normalmente las personas más vulnerables son personas mayores, debido a que los jóvenes están más actualizados en el funcionamiento de la tecnología. También hay delitos relacionados a las los ciberestafas, como la clonación de tarjetas, pero estos no son frecuentes.
2	En relación a la investigación del delito de estafas cibernéticas, ¿cuál es el procedimiento a seguir como investigador y qué rol desempeña usted?	Soy Investigador judicial, y no hay departamentos especializados en la investigación de las estafas informáticas en Aguadulce, pero en la Ciudad de Panamá sí hay un departamento. En los procedimientos de investigación existe parámetros dependiendo al delito, pues,

		hay que observar las características de los hechos o los indicios, como en los casos de llamada telefónicas. Se han dado situaciones en donde la persona ya ha depositado, y todavía siguen en contacto de la víctima, esto se da por la existencia de grupos especializadas en estos delitos. Se dan operaciones a través de citar al victimario a un lugar, o darle seguimiento de las cuentas de bancos para dar el paralelo del estafador. También existe que el que recibe dinero puede ser engañado para recibir una transición, a través de una bonificación o personas que caen con los celulares, ingresas tarjetas, los premios, etc. En una operación grande realizada en esta seccional, fue resolver unos estafadores en Chiriquí. También que la mayoría de estafas son relacionadas con la provincia de Chiriquí, según casos revisados. Algunas de estas estafas son realizadas por los presos, ubicando a través del allanamiento. Nosotros le recomienda a la fiscalía que busque y ayude al IMELCF, pero también realizamos diligencias.

3	¿Qué tan eficiente considera usted que son realizados los procedimientos de investigación para la resolución de las ciberestafas?	No te puedo decir que todos los casos se resuelven, pero sí se tiene vinculado. Siempre hay un imputado, independientemente si el autor principal.
4	¿Cuáles son los obstáculos o limitaciones ante los que se enfrentan durante la ejecución de los procedimientos de investigación judicial en casos de ciberestafa?	Existen limitaciones, como el tiempo, debido a que demora mucho solicitar una diligencia para realizar estas investigaciones, debido a que, si no existiera esto, sería más rápido. Solicitar una aprobación por parte de los bancos, telefónicas, y se debe esperar las respuestas. El conocimiento de parte del investigador para realizar este de delitos o de los dispositivos tecnológicas. Un investigador debe saber de todo, aunque sea básico, debido a que se debe adaptar a la investigación. También la dificultad de aprender sobre las cosas tecnológicas.
5	¿De qué manera se mejorarían los procedimientos de investigación de las estafas informáticas en el corregimiento de Aguadulce?	De pronto asignar a personas en un subdepartamento que se especialicen en este tipo de delitos. Capacitaciones en cuanto a la rama del ciberdelito, debido a que puede ser un tema complicado. Lo mejor es capacitarse en los delitos, debido a que a veces solo se llega con la teoría, también, con el

		tiempo la teoría ayuda a realizar mejores investigaciones.

Cuadro N°3. Entrevista N°2.

N°	Preguntas	Respuestas
1	¿Es frecuente la comisión del delito de estafas informáticas en el corregimiento de Aguadulce? ¿Qué modalidad es la más reportada?	Por lo general, en estadísticas no puedo dar información, debido al por tiempo que llevo en la sección de Aguadulce, pero si se dan bastante frecuente en Aguadulce. Se han dado grupos en donde realizan secuestro telefónico, donde los números que utilizan para realizar estas llamadas, posteriormente los mismos son destruidos. No puedo dar un dato fijo sobre estafas a máquinas en provincias centrales, pero no son tan frecuentes.
2	En relación a la investigación del delito de estafas cibernéticas, ¿cuál es el procedimiento a seguir como investigador y qué rol desempeña usted?	Verificar la existencia del delito, de qué forma se está realizando, y posteriormente conversar con las personas afectadas, seguidos de una reunión previa con la fiscalía para organizar las diligencias dependiendo al tipo de caso. Darte cuenta ante qué situación, del lugar, como y cuando. Previa reunión, buscar cuales son los puntos, o antenas, si son utilizadas los dispositivos tecnológicos, y a que antena se están conectando. Se da un rol general a los investigadores de Aguadulce para estas estafas.

3	¿Qué tan eficiente considera usted que son realizados los procedimientos de investigación para la resolución de las ciberestafas?	Considero que son muy efectivos estos procedimientos de investigación para estos delitos.
4	¿Cuáles son los obstáculos o limitaciones ante los que se enfrentan durante la ejecución de los procedimientos de investigación judicial en casos de ciberestafa?	Las telefónicas de los equipos tardan mucho en dar respuestas, como las compañías de Tigo, más móvil. Siendo los principales. La falta de logística para realizar estas diligencias, como el transporte y dar respuestas, debido a que los centros de atención de las compañías no están en zonas centrales, están en Panamá.
5	¿De qué manera se mejorarían los procedimientos de investigación de las estafas informáticas en el corregimiento de Aguadulce?	Por lo menos, volanteo ante la sociedad para informar sobre estos delitos, como las enseñanzas del manejo y cuidado de las tarjetas. Orientar mucho a la ciudadanía. Coordinar que todas las diligencias en un menor tiempo, y darles prioridad a los casos, por la naturaleza de los mismos. Que el personal este más capacitada para estos delitos, ya que no somos técnicos en estos delitos.

Cuadro N°4. Entrevista N°3

N°	Preguntas	Respuestas
1	¿Es frecuente la comisión del delito de estafas informáticas en el corregimiento de Aguadulce? ¿Qué modalidad es la más reportada?	Es poco frecuente los delitos de estafas, pero la modalidad más reportada son las estafas a través de llamadas que se hacen pasar por otras personas.
2	En relación a la investigación del delito de estafas cibernéticas, ¿cuál es el procedimiento a seguir como investigador y qué rol desempeña usted?	La fiscalía nos comisiona, y posteriormente se da la Verificación de las cuentas, si coinciden con los datos de las personas.
3	¿Qué tan eficiente considera usted que son realizados los procedimientos de investigación para la resolución de las ciberestafas?	Se cumple con los requerimientos de la fiscalía, debido a que se trabaja de acuerdo a los que se les indica.
4	¿Cuáles son los obstáculos o limitaciones ante los que se enfrentan durante la ejecución de los procedimientos de investigación judicial en casos de ciberestafa?	Que las cuentas hayan sido eliminadas, debido a que no se encuentran la página. También se da que son perfile falsos de los victimarios.
5	¿De qué manera se mejorarían los procedimientos de investigación de las estafas informáticas en el corregimiento de Aguadulce?	Informado a las personas sobre este tipo de delitos, y como deben ser utilizadas las redes sociales, debido a que incrementa la criminalidad en estas modalidades.

Cuadro N°5. Entrevista N°4

N°	Preguntas	Respuestas
1	¿Es frecuente la comisión del delito de estafas informáticas en el corregimiento de Aguadulce? ¿Qué modalidad es la más reportada?	Si es frecuente, por lo menos se da un caso por semana, y la modalidad más reportada son las estafas telefónicas.
2	En relación a la investigación del delito de estafas cibernéticas, ¿cuál es el procedimiento a seguir como investigador y qué rol desempeña usted?	Primero se espera la comisión de la fiscalía, y se realizan las investigaciones de campo, como el empadronamiento y entrevistas, así como la individualización del indiciado. Se pone en comunicación con la víctima para recabar información sobre el hecho reportado, posteriormente se investiga quien es el autor del delito, relacionándolo con los números que uso, cuentas y páginas digitales. En casos de estafas en cajeros, la fiscalía hace una solicitud al banco que fue víctima del delito, una vez, el banco aporte la información del victimario se procede a ubicarlos, como la residencia o trabajo. En Aguadulce se dieron aproximadamente unos 6 casos entre 2020 y 2021. El rol como investigador es generalizado de acuerdo a la solicitud de la fiscalía, se

		realizaría una inspección del lugar de los hechos con criminalística, se verifican cámaras para hacerle saber a fiscalía de su existencia.
3	¿Qué tan eficiente considera usted que son realizados los procedimientos de investigación para la resolución de las ciberestafas?	Son bueno y efectivos los procedimientos.
4	¿Cuáles son los obstáculos o limitaciones ante los que se enfrentan durante la ejecución de los procedimientos de investigación judicial en casos de ciberestafa?	Existen muchos obstáculos como la colaboración de la sociedad para la resolución de este delito. Los recursos limitados, como el manejo de las plataformas informáticas de investigación, haciendo lento el proceso. El tiempo disponible a la investigación debido a que existen otras investigaciones al mismo tiempo. Falta recursos por parte del estado para realizar diligencias, como los autos y equipos tecnologías. Falta de máquinas para que todos trabajen al mismo tiempo.
5	¿De qué manera se mejorarían los procedimientos de investigación de las estafas	A través de publicidad a la comunidad para que esta alerta de estos delitos.

	informáticas en el corregimiento de Aguadulce?	Asignándole al investigador las plataformas digitales para la investigación de las ciberestafas.

Cuadro N° 6. Entrevista N°5.

N°	Preguntas	Respuestas
1	¿Es frecuente la comisión del delito de estafas informáticas en el corregimiento de Aguadulce? ¿Qué modalidad es la más reportada?	Si es frecuente, y la modalidad que más se ve es por las llamadas, por el secuestro por parte de los privados de libertad. Otra modalidad constante son las compras en sitios web, donde se deposita el dinero, y no recibían el bien. Como los teléfonos, vehículos y contenderos. Una estafa muy relevante, no hace mucho, fue la estafa por la compra de vehículos del norte.
2	En relación a la investigación del delito de estafas cibernéticas, ¿cuál es el procedimiento a seguir como investigador y qué rol desempeña usted?	En primera instancia la fiscalía los comisiona mediante la plataforma de la SPA, posteriormente se comunican con la víctima para obtener detalles sobre le hecho. En cuanto a la denuncia. Nos apoyamos en el sitio web del hecho, también en ocasiones los autores borran la evidencia. También nos apoyamos de las conversaciones que las personas conservan el teléfono.
3	¿Qué tan eficiente considera usted que son realizados los	En 2021 si fueron efectivos, aunque el tiempo de investigación es lento, así

	procedimientos de investigación para la resolución de las ciberestafas?	como los operativos especiales por medio de la policía. Esto puede llegar al límite de los 6 meses de investigación.
4	¿Cuáles son los obstáculos o limitaciones ante los que se enfrentan durante la ejecución de los procedimientos de investigación judicial en casos de ciberestafa?	Lastimosamente la falta de equipos tecnológicos. A comparación de la ciudad de Panamá. La Velocidad del internet, la solicitud información de los sitios webs, el recurso humano por la cantidad de personas, la logística del equipo para realizar las investigaciones y el poco tiempo de la investigación. También que Las compañías no brindan información sobre las comunicaciones, hasta la fiscalía tiene problemas para obtener la información.
5	¿De qué manera se mejorarían los procedimientos de investigación de las estafas informáticas en el corregimiento de Aguadulce?	Con la educación a los pobladores, y a la vez educar a cada ciudadano que no brinde información. Dar talleres para los padres de familias, para reforzar el conocimiento sobre este tema.

Cuadro N°7. Entrevista N°6.

N°	Preguntas	Respuestas
1	¿Es frecuente la comisión del delito de estafas informáticas en el corregimiento de	Si es uno de los delitos contra el patrimonio que, en los últimos años, 2019 a 2021 ha tenido una gran incidencia.

	Aguadulce? ¿Qué modalidad es la más reportada?	La modalidad más utilizada es por medio de las llamadas telefónicas.
2	En relación a la investigación del delito de estafas cibernéticas, ¿cuál es el procedimiento a seguir como investigador y qué rol desempeña usted?	La noticia criminal se recibe de la fiscalía, ellos a través de la plataforma del SPA, la envían a la DIJ, en donde es asignado un investigador, posteriormente el investigador procede a cumplir las diligencias que el fiscal ordena. Generalmente estas diligencias consisten en ubicar a las personas, los nombres, conversar con las víctimas, se da los análisis telefónicos, observar la activación de las antenas, a través del análisis del modus operandis de los delincuentes. Es al azar el modus operadis de los delincuentes que hacen las estafas por llamadas, marcando hasta encontrar a la víctima. Las víctimas son de todos tipos de estatus, donde por la emoción se dejan llevar por los delincuentes. Mi rol es realizar los análisis telefónicos de este delito.
3	¿Qué tan eficiente considera usted que son realizados los procedimientos de investigación para la resolución de las ciberestafas?	La disposición esta, pero por la falta de herramientas para que el investigador puede realizar su labor.
4	¿Cuáles son los obstáculos o limitaciones ante los que se	Existen muchas limitaciones en la seccional de Aguadulce, como la falta de

	enfrentan durante la ejecución de los procedimientos de investigación judicial en casos de ciberestafa?	un personal adecuada, que sea idóneo en cuanto al manejo de la tecnología, así como herramientas tecnológicas actualizadas, para dar un trabajo eficaz, que den una repuesta positiva la sociedad. Al momento de recibir denuncia hay muchas falacias de datos que son muy importante para aprovechar la situación.
5	¿De qué manera se mejorarían los procedimientos de investigación de las estafas informáticas en el corregimiento de Aguadulce?	Preparando al personal en cuanto a las nuevas modalidades que se estén dando al delito, en cuanto al manejo de la tecnología, la instrucción del profesional, dotándolo de herramientas tecnológicas y mantenimiento. Creando un grupo exclusivo para solucionar este delito, que solo sean encargados para este tipo de delitos. Debido a que el personal más especializado para esa área de delitos.

Cuadro N° 8. Entrevista N°7.

N°	Preguntas	Respuestas
1	¿Es frecuente la comisión del delito de estafas informáticas en el corregimiento de Aguadulce? ¿Qué modalidad es la más reportada?	En los último 2 o 3 años es muy frecuentes, anteriormente no se daba tanto este tipo de delito. Se dan por la facilidad del delincuente en realizar este hecho delictivo, independientemente a la información suministrada a la población.

		La modalidad más reportada en Aguadulce son las estafas telefónicas, con la modalidad de recibir un bien. Los depósitos por lo general son a través de Servicios de envíos como Wester Unión. Otra modalidad nueva, es que las personas se hacen por aduanas, y solicitan a las víctimas que paguen un impuesto por mercancías enviados por un familiar o conocido. Los delincuentes tienen los datos personales para hacerse pasar por alguien, como su nombre, celular, cédula y lugar donde vive.
2	En relación a la investigación del delito de estafas cibernéticas, ¿cuál es el procedimiento a seguir como investigador y qué rol desempeña usted?	Una vez que la persona es estafada, se dirige a la fiscal, interponiendo la denuncia, ya puesta, la fiscalía envía la denuncia a través de la plataforma del SPA. Ya llegada a la seccional, es enviada a mi o al jefe de grupo para proceder a la investigación, revisan los datos de la denuncia para hacer entrevistas a los afectados. Muchas veces el investigador hace que las victimas diga más información relevante para hechos. Por lo general en los casos de estafas siempre se tiene una persona señala. Cuando se tienen a esta persona se obtienen datos de las

		personas, donde con ayuda de la fiscalía se mandan órdenes para retener las cuentas bancarias.
3	¿Qué tan eficiente considera usted que son realizados los procedimientos de investigación para la resolución de las ciberestafas?	Son bastantes buenos, debido a que la general ya se tiene a un indiciado localizado, pero existe poca probabilidad de ser resueltos los casos de estafas cibernéticas si no son conocidos los indiciados.
4	¿Cuáles son los obstáculos o limitaciones ante los que se enfrentan durante la ejecución de los procedimientos de investigación judicial en casos de ciberestafa?	La falta de herramientas, como los sistemas, infraestructura de los dispositivos utilizados, la falta de recursos financieros, logísticos y humanos. Se tiene la disponibilidad, pero el investigador no cuenta con los necesario para realizar los procedimientos.
5	¿De qué manera se mejorarían los procedimientos de investigación de las estafas informáticas en el corregimiento de Aguadulce?	La falta de educación y conocimiento por parte de la sociedad en cuanto a este tema. Orientarlos a que no sean víctimas. Esto no tiene un estatus económico predefinido. Se necesitan los recursos y herramientas para que el investigador pueda realzar su investigación.

Cuadro N°9. Entrevista N°8.

N°	Preguntas	Respuestas
1	¿Es frecuente la comisión del delito de estafas informáticas	Es frecuente. La modalidad más reportada por teléfono, por un premio y en

	en el corregimiento de Aguadulce? ¿Qué modalidad es la más reportada?	donde se debe mandar tarjetas telefónicas. Un caso reciente fueron unas estafas que el autor sacó 37 mil dólares, esta fue realizada por varios días.
2	En relación a la investigación del delito de estafas cibernéticas, ¿cuál es el procedimiento a seguir como investigador y qué rol desempeña usted?	Se da el aviso del Ministerio Publico por medio del SPA, y ya sabiendo el caso se le asigna a una persona, esto debido a que la seccional de Aguadulce no hay secciones para realizar esta investigación. Hay un oficial en cada grupo que supervise la investigación y al mismo tiempo hay otro que verifica los oros grupos.
3	¿Qué tan eficiente considera usted que son realizados los procedimientos de investigación para la resolución de las ciberestafas?	Se llegan al punto de conocer las generales de delincuente, posteriormente pasan a criminalística.
4	¿Cuáles son los obstáculos o limitaciones ante los que se enfrentan durante la ejecución de los procedimientos de investigación judicial en casos de ciberestafa?	La falta de los recursos logísticos, tecnológicos y del recurso humano. La capacitación de la persona
5	¿De qué manera se mejorarían los procedimientos de investigación de las estafas	A través de la educación de la sociedad, de cómo debe ser utilizadas las redes sociales y páginas webs. Verificar al

	informáticas en el corregimiento de Aguadulce?	momento de realizar una compra de un bien. La capacitación de las unidades, no solamente al policía judicial, sino que, a todos, así como los policías preventivos, para que entienda y comprenda en un caso tal pueda darse cuenta que es una ciberestafa.

Cuadro N°10. Entrevista N°9.

N°	Preguntas	Respuestas
1	¿Es frecuente la comisión del delito de estafas informáticas en el corregimiento de Aguadulce? ¿Qué modalidad es la más reportada?	Si es muy frecuente este tipo de delitos, de hecho, nosotros tenemos una jurisdicción bastante amplia desde lo que comprende Coclé a Veraguas, la mayoría de todos los casos por región, Aguadulce este tipo de casos se ve muy poco a comparación de Veraguas y de Penonomé, debido a la cantidad de personas. Las modalidades más reportadas son el pharming, phishing y las estafas por WhatsApp. La mayoría de personas dicen que me hackearon el teléfono, me hackearon el WhatsApp, me hackearon cualesquiera otras cosas, donde las personas cuando reportan en la fiscalía dicen esto, más, sin embargo, esto no es un ataque como tal, sino este tipo de

		herramientas delictivas, como dije en anteriores palabras son estafas aceptadas por el cliente o la personas víctima.
2	En relación a la investigación del delito de estafas cibernéticas, ¿cuál es el procedimiento a seguir como investigador y qué rol desempeña usted?	Nosotros solo tenemos rol de perito, no el de investigador, ni el que lleva la investigación, que en este caso lo lleva la fiscalía, nosotros solamente estamos para acreditar por medio de técnicas y procedimientos que tenemos aquí, en la sección, para poder acreditar una acción, más, sin embargo, como acreditar una acción sino se sabe de dónde viene o de donde sale, donde el rol de nosotros en el proceso solamente sería acredita una información válida de un investigador.
3	¿Qué tan eficiente considera usted que son realizados los procedimientos de investigación para la resolución de las ciberestafas?	Desde mi perspectiva son muy eficientes, bastantes, porque sin esos procedimientos no se podría saber mucho o de repente hacer una investigación a ciegas.
4	¿Cuáles son los obstáculos o limitaciones ante los que se enfrentan durante la ejecución de los procedimientos de investigación judicial en casos de ciberestafa?	Los obstáculos que nosotros tenemos son de adquisición de equipos que están fuera de presupuesto de la institución. Los precios son elevados para soportar la institución, esto nos limita mucho los procesos. Otra seria la falta de recursos humanos, debido a que la cantidad de trabajo es

		muy alta para la cantidad de personas que tenemos aquí.
5	¿De qué manera se mejorarían los procedimientos de investigación de las estafas informáticas en el corregimiento de Aguadulce?	Mejorarían dando docencias a las personas o usuarios de dispositivos, un pequeño conversatorio de repente para instruir a que no caigan en este tipo de estafa.

Cuadro N°11. Entrevista N°10.

N°	Pregunta	Respuesta
1	¿Es frecuente la comisión del delito de estafas informáticas en el corregimiento de Aguadulce? ¿Qué modalidad es la más reportada?	La frecuencia es de media a baja, con una tendencia a alta y las modalidad más reportada que catalogan dentro de delito informático podría ser el phishing, pharming, que es prácticamente una versión mejorada del phishing, donde es más visual y de ingeniería social, porque no es un ataque cibernético, debido a que no usan técnicas más avanzadas de nivel informáticos, como los códigos maliciosos o programas que alteren la integridad de los dispositivos personales de las víctimas y, para mí no llegaría a ese nivel de hackeo, sino de ingeniería social a través de herramientas tecnológicas como lo son las redes sociales, las aplicaciones de mensajerías como WhatsApp, Facebook, etc., muchas estafas que se realizan a través de Facebook por Market Place, donde te ofrecen un terreno a la orilla de la playa

		en cinco mil dólares, y las personas van hacer el depósito en una cuenta y se cumple de estafa, en realidad es poca precaución de las personas a la hora de dar su información, una transacción económica con un persona x, con la cual no tienes información real, donde la ingenuidad de personas y falta de conocimiento a nivel informáticos a la hora de utilizar estos dispositivos. En la mayoría de estos delitos se utiliza el Wester Union, o cualquiera herramienta en donde no sen necesitan identificar y sea difícil vincular con el delincuente.
2	En relación a la investigación del delito de estafas cibernéticas, ¿cuál es el procedimiento a seguir como investigador y qué rol desempeña usted?	La investigación por parte de la fiscalía y la DIJ, y otras entidades que tengan relación con la investigación, nosotros simplemente a petición de la fiscalía o personería, realizamos experticias, asesorías, ya que muchas veces nos llaman y consultan, para esperar que tipo de delito puede ser, donde nos pregunta cosas muy básicas donde podemos estar claros, pero la mayoría de las personas no conocen que puede estar ocurriendo ahí, simplemente dicen, me hackearon el teléfono.
3	¿Qué tan eficiente considera usted que son realizados los procedimientos de	Para mi criterio la eficiencia es lo mayor posible en donde muchas veces toman para sus estadísticas casos que no tienen que ver con delitos informáticos, y lo

	investigación para la resolución de las ciberestafas?	incluyen por el simple hecho de atenderlo. Siempre verificamos cualquier situación, aunque parezca que no sea un delito informático, esto para destacar cualquier situación,
4	¿Cuáles son los obstáculos o limitaciones ante los que se enfrentan durante la ejecución de los procedimientos de investigación judicial en casos de ciberestafa?	La falta de comunicación por parte de las fiscalías y los usuarios, a veces las actas o en las declaraciones las personas omiten información, como el correo, que las personas no se presenten a las diligencias y, dejen a la fiscalía y a nosotros esperando.
5	¿De qué manera se mejorarían los procedimientos de investigación de las estafas informáticas en el corregimiento de Aguadulce?	Difundir información sobre los sitios oficiales de entidades bancarias, que las personas tengan cuidados al momento de acceder a cualquier enlace o cualquier aplicación. Se cree docencia o cultura sobre estemos temas, independientemente de la edad muchas personas acceden a los enlaces o menores que utilizan el teléfono de los padres para solamente con un clic comprar, y no se asegurar que utilizan herramientas para proteger esta información.

Cuadro N° 12. Entrevista N°11.

	Preguntas	**Respuestas**
1	¿Es frecuente la comisión del delito de estafas informáticas	Cada cierto tiempo, cada temporalidad se dan estos tipos de delitos, estas estafas,

	en el corregimiento de Aguadulce? ¿Qué modalidad es la más reportada?	sin embargo, son muchas modalidades las que se establecen, por lo general se mantiene la de una conversación por chat, una conversación por Facebook una aplicación de mensajería en donde llevan a la víctima a ser estafados. Estadísticamente no te puedo dar datos, pero si es muy frecuente, el usuario o seres humanos como tal somos muy propensos a las estafas, todavía existe dentro de la población la ignorancia a temas informáticos, que conllevan a algún tipo de estafa, más cuando se trata de cuentas bancarias, pines, contraseñas, y también que involucren a familiares. Las llamadas telefónicas solamente por utilizar el dispositivo celular, pero dentro del engranaje completo que involucra llevar una estafa por el parte informático, una llamada solo sería un detalle, al final del camino son una serie de herramientas que se utilizan para localizar a alguien, más que nada utilizar la ingeniería social.
2	En relación a la investigación del delito de estafas cibernéticas, ¿cuál es el procedimiento a seguir como investigador y qué rol desempeña usted?	Estos tienen un manual para poder ejecutarlos, en donde cada procedimiento conlleva equipos, conlleva conocimiento, conlleva justificaciones, que nosotros utilizamos la hora de realizar un

		procedimiento a cualquier dispositivo que se presente en la unidad. Nosotros somo la parte técnica cuando los delitos vienen tipificados, analizamos los equipos que se mantienen, pero al final del camino ya esta acción está tipificada, donde nosotros solo realizamos la diligencia. Se levanta la base de datos completa de lo que vayamos a analizar, luego la fiscalía se encarga de buscar que vamos a encontrar. Nuestra investigación se basa en el equipo, lo que se encontré dentro de este equipo va a depender de lo que la fiscalía buscar, como cuentas bancarias, algún chat, alguna fotografía, audio o videos, cualquier elemento que requiere en su investigación.
3	¿Qué tan eficiente considera usted que son realizados los procedimientos de investigación para la resolución de las ciberestafas?	Nosotros solo vemos el análisis, donde con respecto al análisis te puedo decir que los procedimientos que nosotros realizamos están avalados por la institución.
4	¿Cuáles son los obstáculos o limitaciones ante los que se enfrentan durante la ejecución de los procedimientos de	En caso de nosotros, nuestras oficinas están completas, y tenemos el personal para atender las diligencias que se mantienen dentro de una agenda, y los equipos completos para atender cualquier

	investigación judicial en casos de ciberestafa?	tipo de delito, las técnicas y procedimientos son los mismos tanto en la sede principal, como en las otras sedes que nosotros mantenemos en informática forense. Una vez de mantenga la diligencia agendada y se cuenta con los equipos se puede realizar el procedimiento. Lo único que decirte que se puede realizar una diligencia, una limitación, serían por factores externos prácticamente, como la luz, algo en la estructura, fallas en el internet, en cuanto a los equipos siempre se mantienen al día, en las licencias.
5	¿De qué manera se mejorarían los procedimientos de investigación de las estafas informáticas en el corregimiento de Aguadulce?	En cuanto a mejorar todo el tema de las estafas informáticas, sería la capacitación a la ciudadanía, porqué casi la gran mayoría de estafas informáticas, muchas de las personas pecan de inocente, entonces el fallo no es de la parte informática, sino de las personas que son engañadas, y creen en la palabra de alguien le está dando un beneficio.

Finalizando las entrevistas, se obtuvieron diversas perspectivas de los entrevistados sobre los procedimientos de investigación judicial de estafas a través de medios cibernéticos e informáticos.

Sobre los datos generales, se muestra que los encuestados según su sexo la mayoría es masculino representando a un 63 %, y un 37 % era de sexo femenino,

según la edad los encuestados la mayoría tiene entre 31 a 40 años representando un 73 % de los encuestados, con la edad de 20 a 30 años un 9 %, con la edad 41 a 50 un 9 % y con la edad de 51 a 60 un 9 %. Con respecto al título que ostentan los encuestados existen diversos estudios, pero se destaca la Licenciatura e Investigación Criminal y Seguridad, Licenciatura en Redes Informáticas, Licenciatura en Criminalística y Ciencias Forenses, Ingeniería en Sistemas, y la Licenciatura en Derecho y Ciencias Políticas.

Iniciando con las preguntas, la frecuencia en la comisión de los delitos de estafas informáticas en el corregimiento de Aguadulce se le atribuye que es una actividad constante, donde por diversos factores se han observado un aumento exponencial en los últimos años.

Factores como un mayor uso de parte de la sociedad de dispositivos de comunicación e información, la atribución de tareas que anteriormente se realizaban de forma presencial pasaron a un plano virtual, la falta de conocimiento por parte de los usuarios, así como uno de los peligros a la salud más reciente en los últimos años, el COVID-19, que ha obligado a los residentes de Aguadulce adaptarse al uso de los dispositivos para realizar actividades como las compras, los pagos online, el trabajo, la educación y sociabilizar por medio de estos equipos, lo que ha atraído a los delincuentes a realizar o adaptarse a las nuevas tecnologías para obtener un bien patrimonial a través de estos tipos de estafas.

Pero para realizar este tipo de delito, los ciberestafadores en el corregimiento de Aguadulce utilizan principalmente las llamadas y mensajes telefónicos como principal herramienta, esto debido a la facilidad en la comisión de este hecho, el anonimato y los requisitos que se necesitan para llevar a cabo esta investigación. Uso de estos dispositivos para realizar cibersecuestro, extorsiones, hacer falsas identidades de personas o instituciones, y los falsos premios, son las conductas ilícitas de estafa informáticas más comunes en Aguadulce.

Este corregimiento no escapa también de otras modalidades, como el phishing a través de los correos y mensajes instantáneos, el pharming en las páginas de bancos, y el engaño en las ventas de productos en tiendas online. Cabe destacar que en Aguadulce las estafas a equipos como los cajeros, tarjetas o dispositivos similares son prácticamente inexistentes o no son reportadas con las autoridades correspondientes.

Diversos especialistas entrevistados atribuyeron que las ciberestafas reportadas en el corregimiento de Aguadulce no tienen técnicas avanzadas, sino que utilizan la ingeniería social para cometer estos hechos, es decir que utilizan técnicas que parecen inofensivas o no sospechosas, como un mensaje, correos, llamadas, enlaces, etc.

Para hacerle frente a estas modalidades de estafas los investigadores y criminalísticas deben tener un procedimiento adecuado según las características del hecho. Si bien, típicamente la DIJ de Aguadulce empieza la investigación a través del aviso del Ministerio Público sobre el hecho delictivo, el contacto con la víctima para realizar una entrevista y obtener datos, o poder recolectar un posible indicio, para posteriormente iniciar diversas diligencias encaminadas a obtener evidencia que requiere la fiscalía.

Estos procedimientos son los análisis telefónicos, observación de las activaciones de antenas, el análisis de los modus operandi para identificar patrones, así como realizar peticiones a las compañías telefónicas para obtener información sobre la ubicación, o cualquier dato relevante en la investigación de ciberestafas.
En los casos de estafas informáticas las diligencias que realiza en la seccional de Aguadulce son realizadas por cualquier investigador disponible, con la inexistencia de un rol específico para este tipo de casos, adaptándose a los hechos.

De parte de Criminalística de Los Santos, en la sección de Delitos Informáticos, ellos solamente atienden las diligencias que necesitan las fiscalías, estas pueden ser como las asesorías sobre posibles estafas, la realización de experticias y análisis de dispositivo, así como acreditar la información de un investigador, ofreciendo un rol general en todos los casos de delitos informáticos.

¿Son estos procedimientos eficientes para la resolución de las ciberestafas en el corregimiento de Aguadulce?, desde diferentes perspectivas se considera que los procedimientos establecidos en la investigación de estos hechos cumplen su función independientemente se resuelvan los casos de estafa informática en Aguadulce, es decir, que son otros factores que intervienen, ya sea por diferentes limitantes u obstáculos que se encuentran los investigadores o criminalística en el procedimiento.

El equipo de investigación que atiende estas modalidades de ciberestafas está en la disposición de realizar correctamente su labor, siguiendo cada paso o principios que establece toda investigación criminal, pero por la falta de recursos hace que esta labor sea complicada, realizando este procedimiento en un mayor plazo.

Obstáculos y limitaciones que van desde lo más básico como los equipos, hasta el recurso humano. En la seccional de la DIJ de Aguadulce se puede observar estas falencias, debido a que establecer un rol general a los investigadores hace que los mismos tengan deficiencias en ciertas áreas, y con mayor razón en el dominio de tecnologías de información y comunicación, ámbito que en constantes actualización.

No solo la parte del conocimiento informático o la falta de equipos se ven afectados los servidores públicos de la DIJ de Aguadulce, sino aspectos necesarios para realizar toda investigación judicial, como la logística, la demora en obtener información con las compañías de servicios móviles o internet, la poca o inexistente colaboración de la comunidad, el financiamiento por parte del estado

al realizar investigaciones y un recurso muy importante que establece un antes y un después en la investigación de los delitos, y más en las ciberestafas, como el tiempo de investigación y el tiempo en la aprobación de las diligencias.

En el caso de los peritos informáticos en Criminalística de Los Santos, establecen diferentes limitaciones y obstáculos que limitan su trabajo, como son la infraestructura, factores como el servicios de internet, la descoordinación de parte de las fiscalía, el recurso humano y así como la cantidad de los dispositivos, debido a que a que este equipo no solo realiza las diligencias del Corregimiento de Aguadulce, sino que realizan todas las diligencias y procedimientos de diferentes fiscalías de provincias centrales.

Pero con una perspectiva optimista de los entrevistados, algunos cambios pueden mejorar el procedimiento de investigación judicial de las estafas a través de medios cibernéticos e informáticos, afectando positivamente la labor de los investigadores de Aguadulce y de los peritos informáticos de Los Santos.

Estos cambios principalmente van enfocados a la docencia comunitaria del corregimiento de Aguadulce, donde por medio de enseñanzas sobre los riesgos y peligros de las tecnologías de información y comunicación para hacer un uso correcto del mismo, evitando ser víctimas de estas estafas.

Las otras mejoras van enfocadas a la parte investigativa, como la capacitación del cuerpo de investigación de la DIJ de Aguadulce en el manejo de las modalidades de las ciberestafas, las enseñanzas del uso de plataformas investigativas, las mejoras de los equipos informáticos, acompañado de un mantenimiento y actualización constante.

Una de las ideas más relevantes es creación de un equipo que se encargue de los delitos de ciberestafas y otros delitos informáticos, conformado por recursos idóneos para llevar a cabo estos procedimientos judiciales.

4.2 Resultados de la encuesta aplicada en el corregimiento de Aguadulce.

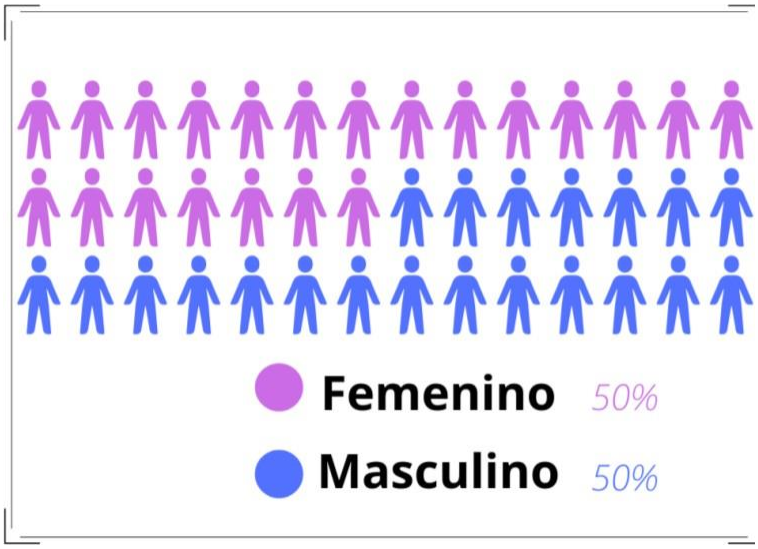
Se presentarán los resultados obtenidos con las encuestas aplicadas a la primera muestra, conformada por los habitantes del corregimiento de Aguadulce. Los resultados de las encuestas fueron:

4.2.1 Datos generales.

Tabla N°2. Personas encuestadas en el corregimiento de Aguadulce, según sexo.

	Cantidad	**Porcentaje %**
Masculino	21	50 %
Femenino	21	50 %

Gráfica N°3. Distribución gráfica de las personas encuestadas, según sexo.

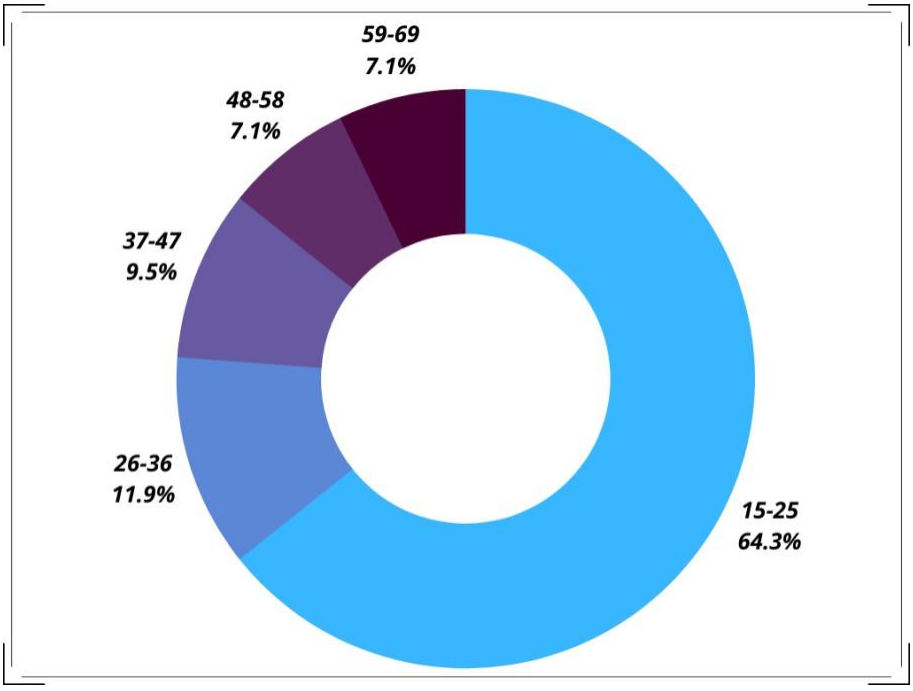


Con respecto a la tabla N°1 y la gráfica N°3, se destaca porcentajes iguales en el sexo de los participantes, con 50 % de género femenino, y de un 50 % correspondientes al género masculino. Observando una participación igual según el sexo, esto con los datos obtenidos en las encuestas.

Tabla N°3. Personas encuestadas en el corregimiento de Aguadulce, según edad.

Edades	Cantidad	Porcentaje %
15-25	27	64,3 %
26-36	5	11,9 %
37-47	4	9,5 %
48-58	3	7,1 %
59-69	3	7,1 %

Gráfica N°4. Distribución gráfica de las personas encuestadas, según edad.

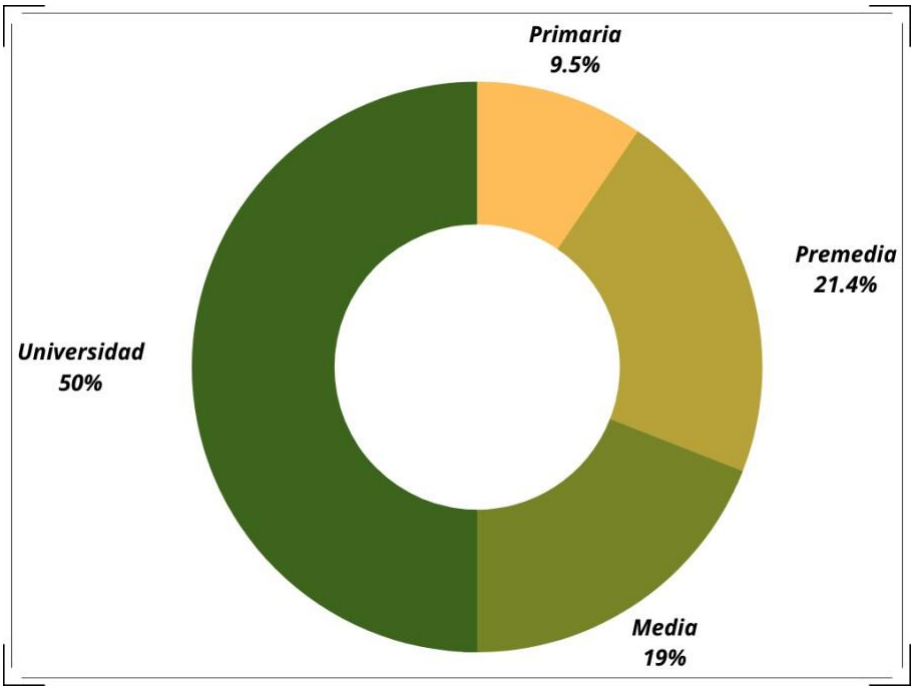


Al terminar la encuesta realizada en el corregimiento de Aguadulce, se evidencia que los participantes en un 64,3 % tienen entre 15 a 25 años, con un 11,9 % tienen entre 26 a 36 años, con un 9,5 % tienen entre 37 a 47 años, seguidos con 7,1 % tienen entre 48 a 58 años, y finalizando con un 7.1 % tienen entre 59 a 69 años. Con esto se puede destacar mayor participación de parte de la población con menor edad, y decreciendo a medida de los años.

Tabla N°4. Personas encuestadas en el corregimiento de Aguadulce, según nivel escolar.

Nivel escolar	Cantidad	Porcentaje %
Primaria	4	9,5 %
Premedia	9	21,4 %
Media	8	19 %
Universidad	21	50 %

Gráfica N°5. Distribución gráfica de las personas encuestadas, según nivel escolar.



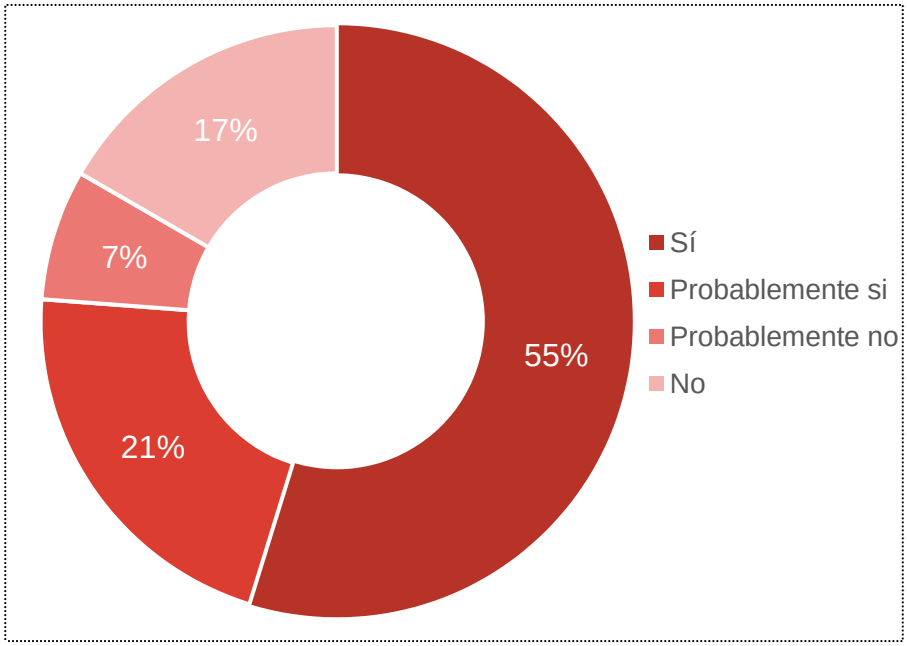
Al terminar la encuesta realizada en el corregimiento de Aguadulce, se evidencia que los participantes en un 50 % tienen un nivel universitario, seguido con un 21,4 % con un nivel de Premedia, con el 19 % de media y finalizando con un 9,5 % están con un nivel primario.

4.2.2 Preguntas

Tabla N°5. Conocimiento sobre las estafas a través de medios cibernéticos o informáticos.

Alternativas	Cantidad	Porcentaje %
Sí	23	55 %
Probablemente sí	9	21 %
Probablemente no	3	7 %
No	7	17 %

Gráfico N°6. Conocimiento sobre las estafas a través de medios cibernéticos o informáticos.

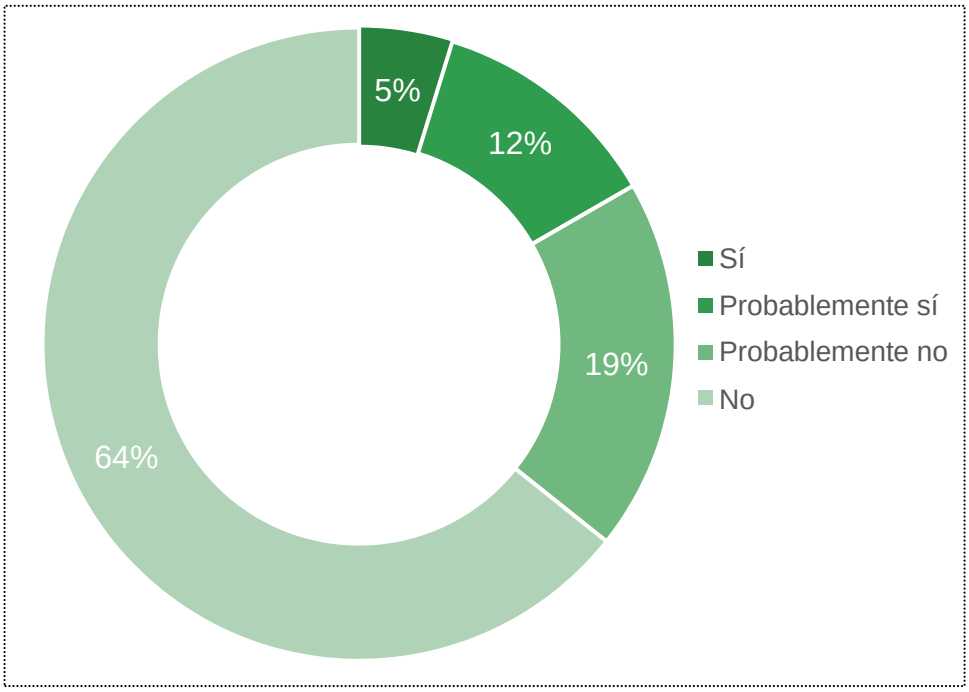


Con respecto al conocimiento de los encuestados sobre este delito, el 55 % de los encuestados seleccionó la alternativa sí, seguidos de un 21 % seleccionaron probablemente sí, con un 17 % la alternativa no, finalizando con un 7 % en un probablemente no. Observando que las estafas a través de medios cibernéticos e informáticos son mayormente conocidas por parte de los participantes del corregimiento de Aguadulce, y que pocos son los que desconocen este fenómeno delictivo.

Tabla N°6. Víctimas de estafas a través de medios cibernéticos e informáticos.

Alternativas	Cantidad	Porcentaje %
Sí	2	5 %
Probablemente sí	5	12 %
Probablemente no	8	19 %
No	27	64 %

Gráfico N° 7. Víctimas de estafas a través de medios cibernéticos e informáticos.

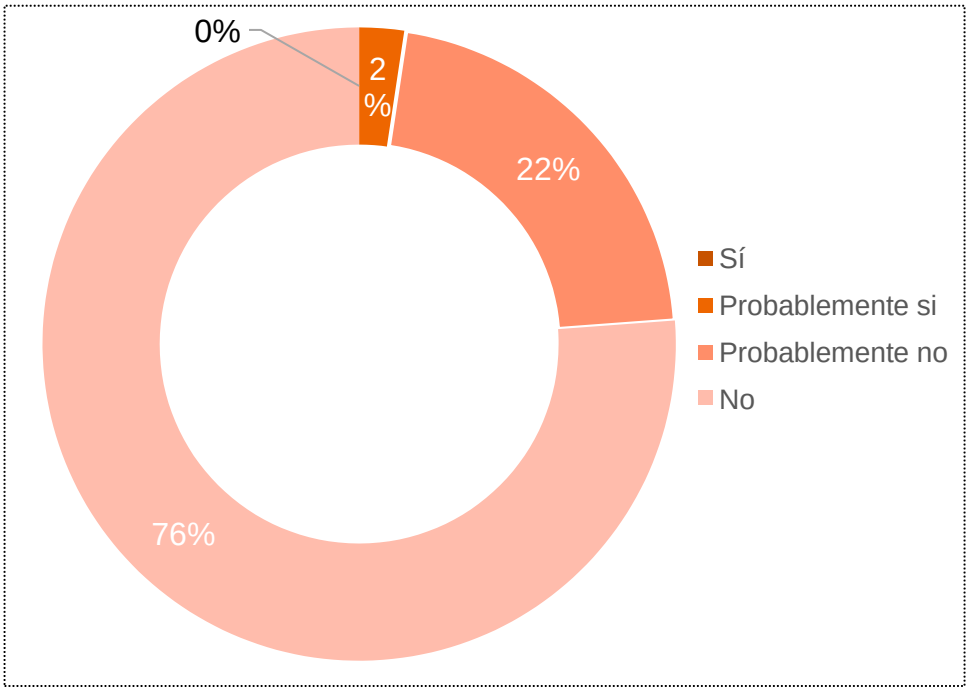


Con respecto a las víctimas de este delito, el 64 % de los encuestados seleccionó la alternativa no, seguidos con un 19 % seleccionaron la alternativa probablemente no, con un 12 % la alternativa probablemente sí, finalizando con un 5 % la alternativa sí. Observando que la mayoría de las respuestas de los encuestado no han sido víctima de las estafas a través de medios cibernéticos o informáticos, y que son muy pocas las que sí fueron víctimas.

Tabla N°7. Denuncias o querellas por estafas a través de medios cibernéticos e informáticos.

Alternativas	Cantidad	Porcentaje %
Sí	0	0 %
Probablemente sí	1	2 %
Probablemente no	9	21 %
No	32	76 %

Gráfica N°8. Denuncias o querellas por estafas a través de medios cibernéticos e informáticos.

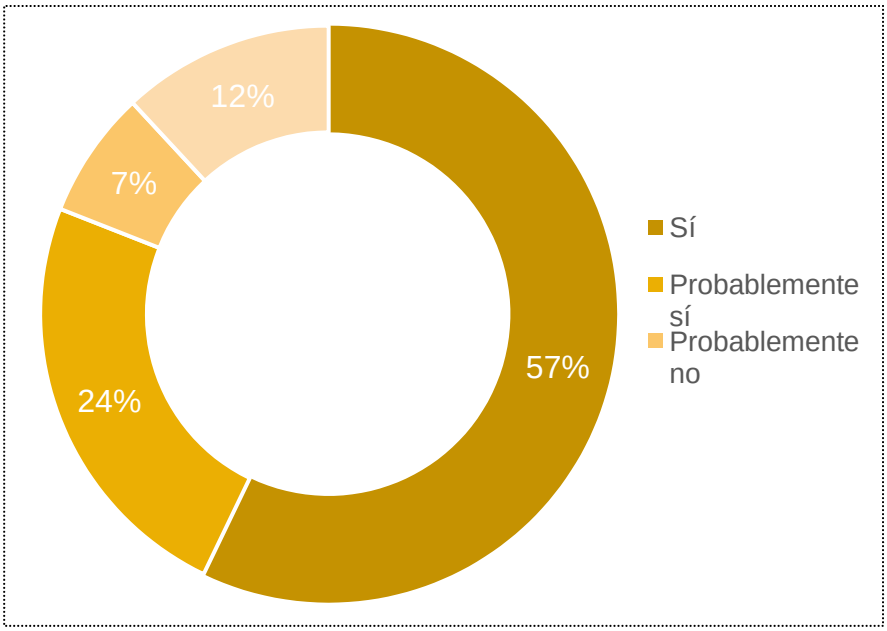


Con respecto a las denuncias o querellas de este delito, el 76 % de los encuestados seleccionó la alternativa no, seguido con un 22 % la alternativa probablemente no, con un 2 % la alternativa sí, y ningún encuestado seleccionó la alternativa sí. Observando que la mayoría de los encuestados no denuncia este comportamiento delictivo, y solo muy pocos o ninguno realizó esta acción.

Tabla N°8. Opinión de las personas encuestadas ante la posibilidad de realizar denuncias en caso de ser una víctima de estafas a través de medios cibernéticos e informáticos.

Alternativas	Cantidad	Porcentaje %
Sí	24	57 %
Probablemente sí	10	24 %
Probablemente no	3	7 %
No	5	12 %

Gráfica N°9. Opinión de las personas encuestadas ante la posibilidad de realizar denuncias en caso de ser una víctima de estafas a través de medios cibernéticos e informáticos.

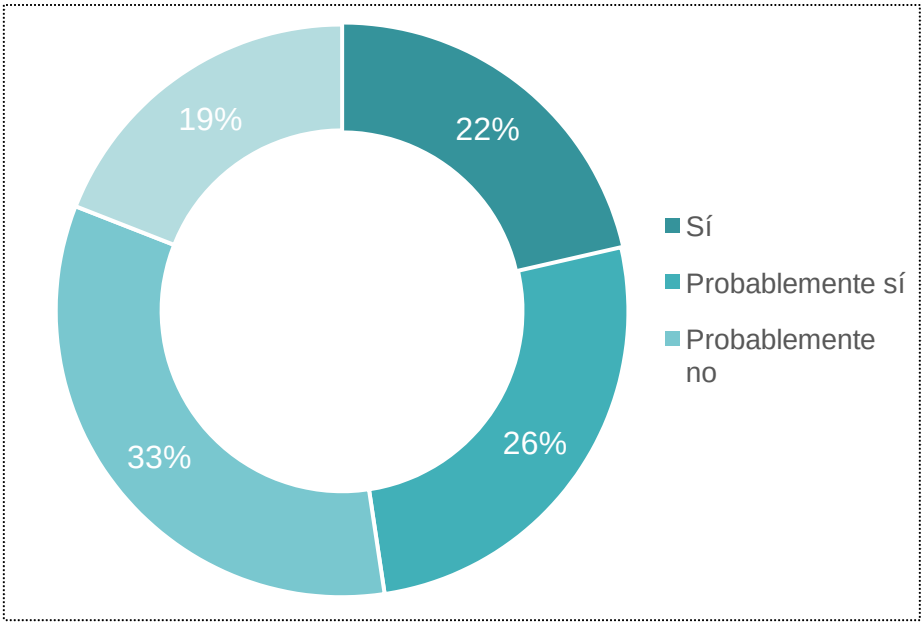


Con respecto a la posibilidad de denunciar al ser víctima de este delito, el 57 % de los encuestados seleccionó la alternativa sí, seguido con un 24 % con la alternativa probablemente sí, con un 12 % la alternativa no, finalizando con un 7 % la alternativa probablemente no. Observando que la mayoría de los encuestados interpondría una denuncia en caso de ser víctimas de las estafas a través de medios cibernéticos e informáticos, y que solo muy pocos no realizarían esta acción.

Tabla N°9. Perspectiva de los encuestados sobre los recursos de las autoridades en los procedimientos de investigación de este delito.

Alternativas	Cantidad	Porcentaje %
Sí	9	21 %
Probablemente sí	11	26 %
Probablemente no	14	33 %
No	8	19 %

Gráfica N°10. Perspectiva de los encuestados sobre los recursos de las autoridades en los procedimientos de investigación de este delito.

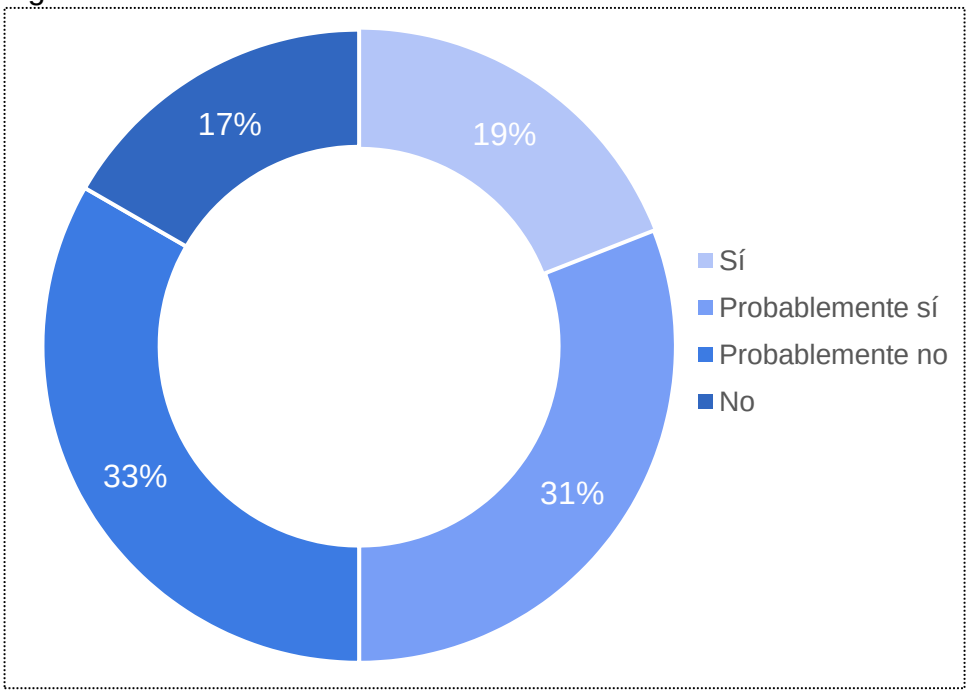


Con respecto a la perspectiva de los recursos de las autoridades de los procedimientos de investigación en este delito, el 33 % de los encuestados seleccionó la alternativa probablemente no, seguidos con un 26 % la alternativa probablemente sí, con un 22 % la alternativa sí, finalizando con un 19 % la alternativa no. Observando que la perspectiva de los encuestados en esta pregunta no está tan dispareja, ofreciendo opiniones distintas sobre los recursos en los procedimientos de investigación en las estafas a través de medios cibernéticos e informáticos.

Tabla N°10. Compromiso de las autoridades en su labor para solucionar de este delito según los encuestados.

Alternativas	Cantidad	Porcentaje %
Sí	8	19 %
Probablemente sí	13	31 %
Probablemente no	14	33 %
No	7	17 %

Gráfica N°11. Compromiso de las autoridades en su labor para solucionar de este delito según los encuestados.

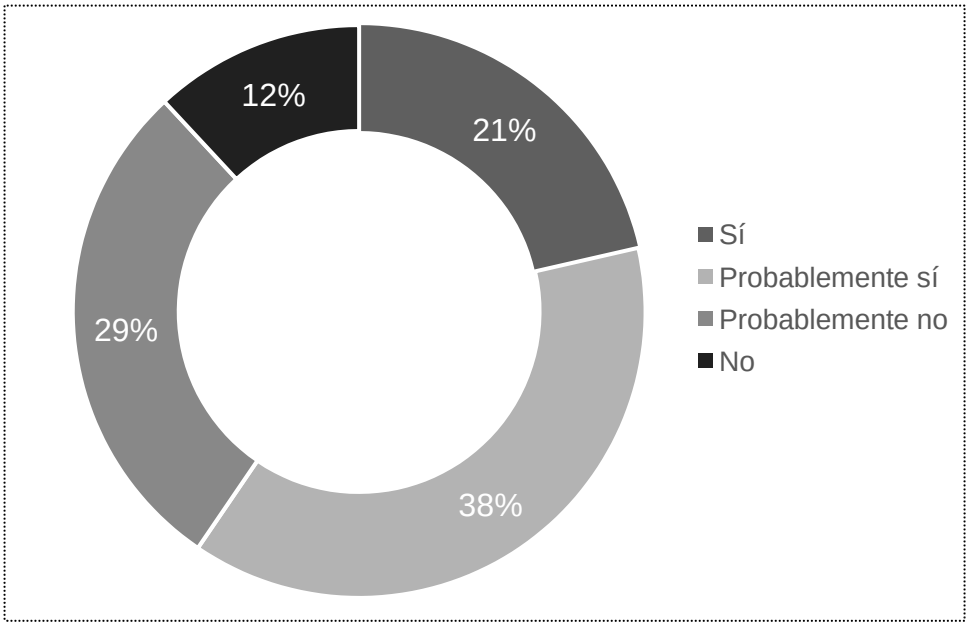


Con respecto al compromiso de las autoridades en su labor, el 33 % de los encuestados seleccionó la alternativa probablemente no, seguidos con un 31 % la alternativa probablemente sí, con un 19 % la alternativa sí, finalizando con un 17 % la alternativa no. Observando en las respuestas una tendencia en las alternativas respuestas: probablemente sí y probablemente, donde los encuestados no están seguros sobre la labor de las autoridades en la solución de las estafas a través de medios cibernéticos e informáticos.

Tabla N°11. Eficacia de la DIJ y de Criminalística en los procedimientos de investigación judicial para solucionar de este delito en el corregimiento de Aguadulce según los encuestados.

Alternativas	Cantidad	Porcentaje %
Sí	9	21 %
Probablemente sí	16	38 %
Probablemente no	12	29 %
No	5	12 %

Gráfica N°12. Eficacia de la DIJ y de Criminalística en los procedimientos de investigación judicial para solucionar de este delito en el corregimiento de Aguadulce según los encuestados.



Con respecto a la eficacia de la DIJ y Criminalística en los procedimientos de este delito, el 38 % de los encuestados seleccionó la alternativa probablemente sí, seguidos con un 29 % la alternativa probablemente no, con un 21 % la alternativa sí, finalizando con un 12 % la alternativa no. Observando que la mayoría de las encuestados considera que los procedimientos de investigación de la DIJ y Criminalística son eficaces, pero no inexistente, otros participantes consideran que los procedimientos son ineficaces.

CONCLUSIONES

Al culminar la investigación se obtuvieron suficientes datos para dar respuestas a los puntos importantes en los aspectos generales de la investigación.

- Los procedimientos de investigación judicial de este delito en el corregimiento de Aguadulce dependerán de la modalidad existente a investigar, pues los mismos son resueltos en su totalidad por Investigadores de la DIJ de Aguadulce o necesita apoyo de peritos informáticos del IMLCF de Los Santos.

- En la Seccional de la DIJ de Aguadulce estos procedimientos son realizados por cualquier investigador, independientemente si tenga o no conocimiento del tema, destacando un protocolo general al inicio, como el recibimiento de la nota del hecho de parte de la fiscalía, la obtención de los datos y detalles de la víctima, el modo, y la fecha del ilícito, para proceder a realizar diligencias más específicas según el tipo de estafa informática.

- Los peritos informáticos del IMELCF de Los Santos tienen una labor diferente a los investigador en los procedimientos, realizando diligencias específicas para apoyar a la investigación; como la certificación de los métodos utilizados por los investigadores; la explicación a los fiscales de las particularidades y evidencias necesarias para comprobar una estafa informática; el revisado, análisis y búsqueda de evidencias en dispositivos para encontrar material probatorio o datos del ciberestafador.

- En cuanto a la eficacia de las autoridades vinculadas en los procedimientos de investigación judicial de las ciberestafas, ofrece un resultado positivo en la resolución de estas modalidades, es decir, que los investigadores y criminalística en el corregimiento de Aguadulce son eficaces, aunque los residentes tienen dudas en cuanto a su compromiso por realizar su labor. (Gráfica N°11, página 123, y Gráfica N°12, Página 124).

- Desde otra perspectiva, en relación a los investigadores judiciales y peritos de informática forense, la eficacia al realizar su labor en la resolución de las estafas informáticas en Aguadulce, depende de los recursos disponibles, ya que, la falta de logística, el recurso humano, el equipo informático obstruyen su desempeño, pues, tienen compromiso al realizar los procedimientos de investigación, adaptándose a las carencias y sobrellevando la situación.

- Estos procedimientos utilizados en la investigación de estafas informáticas en el Corregimiento de Aguadulce, siguen una guía general como cualquier otro delito, pero al realizar diligencias específicas relacionadas a la obtención de material probatorio de información y comunicación, su labor se complica, ocupando la mayor parte del tiempo de los 6 meses de investigación en recibir los permisos necesarios para los datos solicitados.

- Las ciberestafas en este corregimiento, pueden presentarse de diversas modalidades, pero la que más destaca es las de las llamadas telefónicas, un tipo de phishing, técnicas básicas que utiliza la ingeniería social para obtener información de personal, de cuentas de bancos, ofrecer un producto, un servicio o un premio. Otra modalidad en esta localidad es la venta de productos en tiendas online, como las de Instagram, Facebook Marketing y similares, por medio de transacciones de dinero en negocios que no utilizan datos de las personas para recibir el dinero.

- Este fenómeno delictivo va en aumento exponencialmente a través de los años, haciendo que la situación actual en el corregimiento de Aguadulce se presente con recurrencias noticias criminales sobre casos de estafas a través de medios informáticos y cibernéticos, en las cuales se realizan las diligencias pertinentes o procedimientos que permitan descubrir la verdad sobre cada hecho investigado.

RECOMENDACIONES Y LIMITACIONES

Con base en los resultados obtenidos de la investigación, se hace necesario exponer algunas recomendaciones importantes en relación al tema estudiado:

- Es necesario implementar un cambio en la seccional de la DIJ de Aguadulce para hacer frente a estos delitos, con la formación de un equipo investigativo capacitado para realizar investigaciones de delitos informáticos como las ciberestafas. También realizar mejoras en los equipos tecnológicos, acompañado de constante mantenimiento de los mismos, así como de aplicaciones que ayuden en la gestión y resolución de este delito.

- Hacer que los investigadores de Aguadulce tengan prioridad en un solo caso, principalmente en casos informáticos como las ciberestafas, para mantener una gran calidad y eficiencia en los procedimientos de investigación. Esto se puede realizar a través de la adquisición de recursos humanos, logísticos, y tecnológicos, con la inversión de las autoridades del estado en beneficio de la población.

- Con respecto a la sección de delitos informáticos del IMELCF de Los Santos, considero establecer más personal experto en esta área para sobrellevar las diligencias correspondientes, y también realizar un acompañamiento más cercano a los procedimientos de investigación.

- Hacer que las diligencias para obtener información sobre las comunicaciones o datos personales de los clientes de las compañías telefónicas o cualquier base de datos pública y privada necesaria para un procedimiento, sea más rápida y sencilla, debido a que esta parte es la que ocupa mayor tiempo en las investigaciones de estafas informáticas.

- Realizar capacitaciones a los investigadores judiciales sobre el uso de las nuevas tecnologías, técnicas y aplicaciones de los nuevos delitos informáticos, y principalmente las modalidades de la ciberestafa, como los diferentes tipos de phishing y pharming, esto con el objetivo de que sean capaces de identificar y clasificar estos delitos para comprender ampliamente el panorama de estas investigaciones.

- También realizar talleres, conferencias y volanteo a los residentes del corregimiento de Aguadulce, con el fin de crear prevención sobre las estafas informáticas, y las modalidades más comunes que utilizan los ciberestafadores en esta localidad. Con ayuda de medios de difusión como las redes sociales se puede hacer que este mensaje llegue a las personas del corregimiento.

Limitaciones

- La actual Pandemia representó un obstáculo en la realización de la investigación, debido a que los procedimientos, la obtención de información y otros aspectos relevantes, fueron un proceso más lento, debido a las medidas de bioseguridad de estas instituciones.

- La falta de tiempo, recursos y equipo tecnológico para realizar la estructuración y desarrollo de la investigación, conforme a lo establecido en el nuevo manual de trabajo de grado de la UDELAS.

REFERENCIAS BIBLIOGRÁFICAS E INFOGRAFÍAS

Alvarado, A., (29 de junio, 2021). Estafa y extorsión mediante el ciberdelito se han disparado en Panamá, no se convierta en otra víctima. La Verdad Panamá. https://www.laverdadpanama.com.pa/estafa-y-extorsion-mediante-el-ciberdelito-se-han-disparado-en-panama-no-se-convierta-en-otra-victima/

Álvarez R., (17 de diciembre, 2020) Delitos con el uso de tecnología han incrementado en un 130%. Metro Libre. https://www.metrolibre.com/nacionales/189326-delitos-con-el-uso-de-tecnolog%C3%ADa-han-incrementado-en-un-130.html

Álvarez, J., (20 de febrero, 2020). Delito de producción y difusión de imágenes de abuso sexual infantil: breves aproximaciones a la legislación vigente. https://www.erreius.com/actualidad/12/penal-y-procesal-penal/Nota/629/delito-de-produccion-y-difusion-de-imagenes-de-abuso-sexual-infantil-breves-aproximaciones-a-la-legislacion-vigente

Álvarez, R., (2 de junio, 2021). 'Jackpotting', el hack que permite vaciar cajeros automáticos a una velocidad de 40 billetes cada 23 segundos. https://www.xataka.com/seguridad/jackpotting-el-hack-que-permite-vaciar-cajeros-automaticos-a-una-velocidad-de-40-billetes-cada-23-segundos

Arispe, C., Yangali, J., y Guerrero M., (2020). La investigación científica: una aproximación para los estudios de posgrado. Universidad Internacional del Ecuador, Guayaquil. https://elibro.net/es/ereader/udelas/171469

ASALE, R., & RAE. (2020). Diccionario de la lengua española RAE - ASALE. “Diccionario de La Lengua Española” - Edición Del Tricentenario. https://dle.rae.es

Avast Academy Team. (7 de noviembre, 2016). Botnet. https://www.avast.com/es-es/c-botnet

Balmaceda, G., (2011). El delito de estafa: una necesaria normativización de sus elementos típicos. Revista Estudios Socio-Jurídicos 13 (2). http://www.scielo.org.co/pdf/esju/v13n2/v13n2a07.pdf

Balmacedas, G., (2011). El delito de estafa informática en el derecho europeo continental. Revista de Derecho y Ciencias Penales (17). https://dialnet.unirioja.es/descarga/articulo/4200389.pdf

Balmaceda, G., (2016). El delito de estafa. Universidad de los Andes. https://elibro.net/es/ereader/udelas/118325?page=83

Barreiro, F., (8 de noviembre, 2017). El país, top 10 en el ranking de phishing. El Economista. https://eleconomista.com.ar/negocios/el-pais-top-10-ranking-phishing-n16239

Barrera, S., (2019). CIBERPOL. Metodología para la investigación del cibercrimen. Máster Universitario. Universidad Internacional de la Rioja. https://reunir.unir.net/bitstream/handle/123456789/10060/Barrera%20Ib%C3%A1%C3%B1ez%2C%20Silvia.pdf?sequence=1&isAllowed=y

Barrio, M., (2017). Ciberdelitos: amenazas criminales del ciberespacio. Editorial Reus. https://elibro.net/es/ereader/udelas/46673

Beermann, K., (2018). La problemática de la interceptación informática en Panamá. Tesis de grado. Universidad de Panamá. http://up-rid.up.ac.pa/1683/1/kurt%20beermann.pdf

Belcic, I., (20 de septiembre, 2021). Guía esencial del phishing: cómo funciona y cómo defenderse. https://www.avast.com/es-es/c-phishing#gref

Bello, E., (1 de julio, 2020). Ciberseguridad: Tipos de ataques y en qué consisten. https://www.iebschool.com/blog/ciberseguridad-ataques-tecnologia/

Blog de CEUPE. (13 de julio, 2020). Todo lo que se debe saber de virus informáticos. CEUPE. https://www.ceupe.com/blog/todo-lo-que-se-debe-saber-virus-informaticos.html

Buffete Campos & Asociados. (18 de febrero, 2020). Estafa informática [Archivo de video]. https://www.youtube.com/watch?v=DvsDcP6-sYg

Carque, J., (2016). Nuevas tecnologías, policía y prevención del Delito. Tesis de grado. Universitat Jaume I. http://repositori.uji.es/xmlui/handle/10234/161486

Castillo, I., (30 de mayo, 2021). Los elementos del delito de estafa. Mundo Juridico.https://www.mundojuridico.info/los-elementos-del-delito-de-estafa/

Código Penal de la República de Panamá. (2007) Asamblea Nacional de Panamá. https://ministeriopublico.gob.pa/wp-content/uploads/2016/09/codigo-penal-2016.pdf

Constitución Política de la República de Panamá. (2004). Gaceta Oficial 25176. Asamblea Legislativa. https://pdba.georgetown.edu/Constitutions/Panama/vigente.pdf

Convenio Nº185 (2001). Convenio sobre la ciberdelincuencia. Consejo de Europa. https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

Coriat, A., (19 de mayo, 2021). Cibercrimen se dispara, aumentó en un 344% en los últimos cinco años. La Estrella de Panamá. https://www.laestrella.com.pa/nacional/210519/cibercrimen-dispara-aumento-344-ultimos

Córtez, L., Haydee, A. y Lagos, M., (2020) Nuevas tecnologías en la investigación criminal - Aportes de la Informática a la Criminalística y las Ciencias Forenses. https://repository.unilibre.edu.co/bitstream/handle/10901/19597/Nuevas%20tecnologias%20en%20la%20investigacion%20criminal%20aportes%20de%20la%20Informatica.pdf?sequence=1&isAllowed=y#page=158

Detención provisional para un ciudadano, por delito de estafa. (28 de enero, 2019). Noticias emitidas por el Departamento de Información y Relaciones Públicas. https://ministeriopublico.gob.pa/detencion-provisional-para-un-ciudadano-por-el-delito-de-estafa/

Espinoza, N., (25 de febrero, 2018)., ¿Cuál es el «iter criminis» en el delito de estafa que el operador jurídico debe valorar?. La Pasión por el Derecho. https://lpderecho.pe/iter-criminis-delito-estafa-operador-juridico-valorar/

Fernández D. y Martínez G., (2020). Ciberdelitos. Ediciones Experiencia. https://elibro.net/es/ereader/udelas/167811

Fratti, S., (2018). Panamá: un país con la necesidad de una legislación sobre cibercrimen. https://www.ipandetec.org/wp-content/uploads/2018/08/IPANDETEC-Budapest-final-DD.pdf

García, I., y Machado, M., (2018). El delito de estafa cometido por medios informáticos. Tesis de licenciatura. Universidad de El Salvador, Salvador. ihttp://ri.ues.edu.sv/id/eprint/19984/1/EL%20DELITO%20DE%20ESTAFA/%20COMETIDO%20POR%20MEDIOS%20INFORMATICOS.pdf

Giménez, A., (6 de marzo, 2014). Panamá firma pacto mundial contra la ciberdelincuencia. Panamá América. https://www.panamaamerica.com.pa/economia/panama-firma-pacto-mundial-contra-la-ciberdelincuencia-4600

Godoy, J., (2020). Regulaciones panameñas a los delitos informáticos que afectan los Sistemas de Información Contables Administrativos (SICA). Revista Científica Orbis Cógnita 4(1). https://revistas.up.ac.pa/index.php/orbis_cognita/article/view/1109/925

Gómez, A., (30 de enero, 2020). ¿En qué consiste la estafa en Internet? [Archivo de video]. https://www.youtube.com/watch?v=yAZLeDeL7dY

González E., (2019). Factor familiar asociado a la delincuencia juvenil en la Barriada El Alba. Tesis de licenciatura. UDELAS. http://repositorio2.udelas.ac.pa/bitstream/handle/123456789/295/EGonzalez.pdf?sequence=1&isAllowed=y

González, J., (2011). Estrategias legales frente a las ciberamenazas. Cuaderno de estrategias (149). https://dialnet.unirioja.es/servlet/articulo?codigo=3837283

González, M., (2014). Fraudes en internet y estafa informática. Máster Universitario. Universidad de Oviedo. https://digibuo.uniovi.es/dspace/bitstream/handle/10651/27824/TFM_Gonzalez%20Suarez,%20Marcos.pdf;jsessionid=304AA4E0F818F4CA561226BCBA07D26B?sequence=3

Grupo Ático34. (18 de agosto, 2016). Suplantación de identidad, te puede ocurrir a ti. https://protecciondatos-lopd.com/empresas/suplantacion-de-identidad/

Gutiérrez, M., (2015). Fraude informático y estafa. Ministerio de Justicia de España. https://elibro.net/es/ereader/udelas/52457?page=33

Guzmán, K., (7 de julio, 2021). ESET advierte sobre las estafas más comunes en Facebook y cómo evitarlas. Radio Panamá. https://www.radiopanama.com.pa/noticias/tecnologia/eset-advierte-sobre-las-estafas-mas-comunes-en-facebook-y-como-evitarlas/20210705/nota/4148906.aspx

Harán, J., (14 de febrero, 2019). Estafas en apps y sitios de citas online: cuando el amor se convierte en una pesadilla. Welivesecurity. https://www.welivesecurity.com/la-es/2019/02/14/estafas-apps-sitios-citas-online/

Harán, J., (22 de septiembre, 2020a). Estafa telefónica: se hacen pasar por la ANSES para obtener las credenciales del home banking. https://www.welivesecurity.com/la-es/2020/09/22/estafa-telefonica-hacen-pasar-por-anses-obtener-credenciales-home-banking/

Harán, J., (25 de noviembre, 2020b). Crece el ecommerce y aumentan las estafas y los incidentes de seguridad. https://www.welivesecurity.com/la-es/2020/11/25/crece-ecommerce-aumentan-estafas-incidentes-seguridad/

Hernández, R., Fernández, C. y Baptista P., (2014). Metodología de la investigación sexta edición. http://observatorio.epacartagena.gov.co/wp-content/uploads/2017/08/metodologia-de-la-investigacion-sexta-edicion.compressed.pdf

Instituto de Investigación Jurídica de la UNAM. (2013). Aspectos Introductorios de la Investigación Criminal en el Sistema Penal Acusatorio. México: UNAM. https://archivos.juridicas.unam.mx/www/bjv/libros/7/3454/5.pdf

Instituto Nacional de Estadística y Censo. (18 de noviembre, 2013) Estimación y proyecciones de la población total del país, por provincia, comarca indígena, distrito y Corregimiento, según sexo y edad: años 2010-20. https://www.inec.gob.pa/publicaciones/Default3.aspx?ID_PUBLICACION=556&ID_CATEGORIA=3&ID_SUBCATEGORIA=10

Jiménez, T., (12 de septiembre, 2020). Ciberdelincuentes arrecian sus ataques durante la pandemia. Panamá América.

https://www.panamaamerica.com.pa/tecnologia/ciberdelincuentes-arrecian-sus-ataques-durante-la-pandemia-1171926

Juárez, E., (26 de julio, 2017). Conozca cuáles son los principales fraudes financieros. El Economista; El Economista. https://www.eleconomista.com.mx/finanzaspersonales/Conozca-cuales-son-los-principales-fraudes-financieros-20170726-0139.html

Kulikova, T., y Shcherbakova, T., (5 de agosto, 2021). Spam y phishing en el segundo trimestre de 2021. https://securelist.lat/spam-and-phishing-in-q2-2021/94713/

Lago, V., (2017)., La práctica de la investigación criminal: Inspección Técnico Ocular (ITO). https://www.editorialreus.es/libros/la-practica-de-la-investigacion-criminal-inspeccion-tecnico-ocular-ito/9788429019841/

Leal J., (2011). Técnicas policiales y judiciales en la investigación criminal.: Docta Ignorancia Digital: Revista de pensamiento y análisis 2(2). https://dialnet.unirioja.es/descarga/articulo/3763113.pdf

Lemaitre, R., (12 de mayo, 2018). Tema de la semana: Estafa Informática [Archivo de Video]. https://www.youtube.com/watch?v=Su8JhbiCzq0

Ley 69. (2007). Gaceta Oficial Digital No. 25949. Órgano Legislativo de Panamá. https://www.gacetaoficial.gob.pa/pdfTemp/25949/8238.pdf

Leyton, J., (2014). Los elementos típicos del delito de estafa en la doctrina y jurisprudencia contemporáneas. Ars Boni et Aequi 10(2). http://www.ubo.cl/icsyc/wp-content/uploads/2014/12/123161.pdf

López I., (2016). Aplicación de las Tecnologías de la Información y de la Comunicación a la investigación Criminal 13(2). http://www.iiisci.org/journal/pdv/risci/pdfs/CA489BC16.pdf

López, P., y Fachelli, S., (2015). Metodología de la investigación social cuantitativa. https://ddd.uab.cat/pub/caplli/2017/185163/metinvsoccua_cap2-4a2017.pdf

Loredo, J., y Ramírez, A., (2013). Delitos informáticos: su clasificación y una visión general de las medidas de acción para combatirlo. CELERINET 2.

http://celerinet.fcfm.uanl.mx/index.php/revistero/10-revistero/8-celerinet-ano-1-vol-2

Mariana, S., (2015). El Phishing. Trabajo final de Grado. Universidad Jaume I. http://repositori.uji.es/xmlui/bitstream/handle/10234/127507/TFG_Leguizam%C3%B3n_Mayra.pdf?sequence=1

Martínez, L., Leyva, M., Feliz, L., et al. (2014). Virtualidad, ciberespacio y comunidades virtuales. Red Durango de Investigadores Educativos, A. C. http://www.upd.edu.mx/PDF/Libros/Ciberespacio.pdf

McAfee. (19 de marzo, 2021). Ejemplos de phishing: cómo detectar un correo de phishing. https://www.mcafee.com/blogs/languages/espanol/ejemplos-de-phishing-como-detectar-un-correo-de-phishing/

Morellas, D., (2013). Introducción a la criminología. Revista De Derecho (8). https://doi.org/10.5377/derecho.v0i8.978

Moreno, R., (17 de junio, 2020). Ciberestafas [Listado completo de delitos informáticos y cómo evitarlos]. https://mcsocialmedia.com/ciberestafas-listado-completo-delitos-informaticos-como-evitarlos/

Norton LifeLock Inc. (2021). Cómo evitar las estafas en línea. https://lam.norton.com/internetsecurity-online-scams.html

Ochoa, C., (15 de abril, 2015). Muestreo probabilístico: muestreo estratificado. Netquest.com. https://www.netquest.com/blog/es/blog/es/muestreo-probabilistico-muestreo-estratificado

Ospina Abogados. (10 de septiembre, 2021). ¿Cuáles son las estafas informáticas más destacadas y cómo prevenirlas?. https://ospina.es/cuales-son-las-estafas-informaticas-mas-destacadas-y-como-prevenirlas/

Owaida, A., (19 de marzo, 2021). Denuncias de víctimas de delitos informáticos aumentaron 69% en 2020, informó el FBI. https://www.welivesecurity.com/la-es/2021/03/19/denuncias-victimas-delitos-informaticos-aumentaron-2020

Pagnotta, S., (28 de junio, 2017). Las víctimas de ciberataques perdieron 1,33 mil millones de dólares en 2016. Welivesecurity.

https://www.welivesecurity.com/la-es/2017/06/28/victimas-ciberataques-millones-dolares/

Pastorino, C., (17 de diciembre, 2017). Convenio de Budapest: beneficios e implicaciones para la seguridad informática. Welivesecurity. https://www.welivesecurity.com/la-es/2017/12/06/convenio-budapest-beneficios-implicaciones

Pérez, J., y Gardey, A., (2021). Definición de Error. https://definicion.de/error/

Pérez, L., Pérez, R., y Seca, M., (2020). Metodología de la investigación científica. Editorial Maipue. https://elibro.net/es/ereader/udelas/138497?page=213.

Pesantes, L, Valarezo, L., y Vilela, W., (2019). Importancia de la investigación judicial y criminalística en la determinación de la veracidad del delito. Universidad y Sociedad 11(4). https://rus.ucf.edu.cu/index.php/rus/article/view/1328/1354

Policía Nacional de Panamá. (6 de febrero, 2021). “Con el lanzamiento de la segunda parte de la campaña #ElCiberDelitoEsReal le hacemos frente a las modalidades que se enfocan en la compra y venta de productos, a través de plataformas electrónicas (e-commerce) y que está afectando a particulares y comerciantes” [Tuit]. https://t.co/5PjRoQt9Kn

Pons, V., (2017). Internet, la nueva era del delito: ciberdelito, ciberterrorismo, legislación y ciberseguridad. URVIO, Revista Latinoamericana de Estudios de seguridad (20). https://www.redalyc.org/jatsRepo/5526/552656641007/552656641007.pdf

Quevedo, J., (2017) Investigación y pruebas del ciberdelito. Tesis de doctorado. Universidad de Barcelona. https://www.tdx.cat/bitstream/handle/10803/665611/JQG_TESIS.pdf?sequence=1&isAllowed=y

Quispe, Y., (2020). Estafa en el derecho romano. Monografía. Universidad Nacional del Altiplano. https://derecho.unap.edu.pe/temis/files/original/1/3/TRABAJO_MONOGRA_FICO_DE_ESTAFA-YULIZA.pdf#pdfjs.action=download

Rayon., M., y Gómez., J., (2014). Cibercrimen: particularidades en su investigación y enjuiciamiento. Anuario jurídico y económico escurialense (47). https://dialnet.unirioja.es/servlet/articulo?codigo=4639646

Resolución N° DG-173-19 (2019). Gaceta Oficial Digital No. 29069. Ministerio Publico. http://www.imelcf.gob.pa/wp-content/uploads/2021/06/DSP-Publicado-2020-Gaceta-N-29069-15-de-julio-2020.pdf

Rodríguez, V., (6 de julio, 2020). Delitos informáticos aumentan un 200% durante la pandemia. El Siglo. http://elsiglo.com.pa/panama/delitos-informaticos-aumentan-200-durante-pandemia/24159864

Rohde, M., (16 de junio, 2021). Evita a los estafadores en internet al buscar empleo en línea. AARP. https://www.aarp.org/espanol/dinero/estafas-y-fraudes/info-2021/evita-enganos-al-buscar-empleo-en-internet.html

Ruíz, C., (29 de diciembre, 2021). Aprehenden a presuntos estafadores. Noticias emitidas por el Departamento de Información y Relaciones Públicas. https://ministeriopublico.gob.pa/aprehenden-a-presuntos-estafadores/

Sánchez, G., (2012). Delitos en internet: clases de fraudes y estafas y las medidas para prevenirlos. Boletín de Información (324). https://doi.org/https://dialnet.unirioja.es/descarga/articulo/4198948.pdf

Sánchez, J., (28 de mayo, 2016) Patrimonio. Economipedia. https://economipedia.com/definiciones/patrimonio.html

Sevilla, T., (2012). Victimología. Editorial Seguridad y Defensa. https://elibro.net/es/ereader/udelas/119428?page=25.

Torres, I., (4 de octubre, 2019). ¿Cuál es la diferencia entre proceso y procedimiento?. Ive Consultores. https://iveconsultores.com/diferencia-entre-proceso-y-procedimiento/

Trejo, K., (2021). Fundamentos de metodología para la realización de trabajos de investigación. Editorial Parmenia, Universidad La Salle México. https://elibro.net/es/ereader/udelas/183470

Universidad Internacional de Valencia. (2021). Por qué es importante la ciberseguridad. https://www.universidadviu.com/pe/actualidad/nuestros-expertos/por-que-es-importante-la-ciberseguridad

Westreicher, G., (30 de marzo, 2020). Estafa. Economipedia. https://economipedia.com/definiciones/estafa.htm

ANEXOS

ANEXO N° 1

CUESTIONARIO DE ENTREVISTA

Universidad Especializada de las Américas

Extensión Coclé

Facultad de Educación Social y Desarrollo Humano

Licenciatura en Investigación Criminal y Seguridad

Entrevista dirigida a miembros de la DIJ y el IMELCF relacionados a los procedimientos de investigación judicial en el corregimiento de Aguadulce en los casos de estafas a través de medios cibernéticos o informáticos.

La recolección de información realizada con esta herramienta, es relevante para cumplir los objetivos planteados en la tesis denominada como, procedimientos en la investigación judicial de estafas a través de medios cibernéticos o informáticos, llevada a cabo en el año 2020 y los primeros seis meses del 2021.

Para mayor comodidad en la entrevista, se utilizarán los términos de estafas informáticas, ciberestafas, estafas en línea o estafas tecnológicas para referirse a las estafas a través de medios cibernéticos o informáticos. Todos los datos recolectados serán tratados con responsabilidad y discrecionalidad.

1. Datos Generales

Nombre:_____Sexo:_____Edad:_____

Título: _____

2. ¿Es frecuente la comisión del delito de estafas informáticas en el corregimiento de Aguadulce? ¿Qué modalidad es la más reportada?

3. En relación a la investigación del delito de estafas cibernéticas, ¿cuál es el procedimiento a seguir como investigador y qué rol desempeña usted?

4. ¿Qué tan eficiente considera usted que son realizados los procedimientos de investigación para la resolución de las ciberestafas?

5. ¿Cuáles son los obstáculos o limitaciones ante los que se enfrentan durante la ejecución de los procedimientos de investigación judicial en casos de ciberestafa?

6. ¿De qué manera se mejorarían los procedimientos de investigación de las estafas informáticas en el corregimiento de Aguadulce?

ANEXO N° 2

CUESTIONARIO DE ENCUESTA

PROCEDIMIENTOS EN LA INVESTIGACIÓN JUDICIAL DE ESTAFAS A TRAVÉS DE MEDIOS CIBERNÉTICOS O INFORMÁTICOS

Licenciatura en Investigación criminal y Seguridad.

Procedimientos en la Investigación Judicial de Estafas a través de medios cibernéticos o informáticos

Esta encuesta tiene el propósito de recabar información acerca de la Tesis de Grado: Procedimientos en la Investigación Judicial de Estafas a través de medios cibernéticos o informáticos.

🔍Objetivo General:
Analizar los procedimientos utilizados para la investigación de las estafas a través de medios cibernéticos o informáticos en Aguadulce.

📄Nota. Los resultados serán utilizados únicamente con fines académicos y de estricta confidencialidad.

💻Datos:
Las estafas a través de medios cibernéticos o informáticos, o también conocidas como las estafas en línea, estafas tecnológicas o ciberestafas, son aquellas que realizan las conductas de una estafa tradicional, pero con el uso de equipos informáticos para lograr obtener un bien patrimonial de un tercero o de un sistema. Ejemplos como el phishing, estafas a cajeros, el envió de dinero a terceros sin recibir un bien económico, etc.

luis.perez.1@udelas.ac.pa Cambiar de cuenta

*Obligatorio

Correo *

Tu dirección de correo electrónico

Datos generales

Sexo *

- ○ M
- ○ F

Edad *

- ○ 15-25
- ○ 26-36
- ○ 37-47
- ○ 48-58
- ○ 59-69

Nivel escolar *

- ○ Primaria
- ○ Premedia
- ○ Media
- ○ Universidad

Preguntas *

4	3	2	1
Sí	Probablemente si	Probablemente no	No

	4	3	2	1
¿Conoce sobre las estafas a través de medios cibernéticos e informáticos?	○	○	○	○
¿Ha sido usted víctima de estafas a través de medios cibernéticos e informáticos?	○	○	○	○
¿Ha realizado alguna denuncia o querella por estafas a través de medios cibernéticos e informáticos?	○	○	○	○
¿Pondría usted alguna denuncia o querella en el hipotético caso de ser una víctima del delito de estafas a través de medios cibernéticos e informáticos?	○	○	○	○

¿Considera usted que las autoridades tienen los recursos para realizar los procedimientos de investigación judicial en delitos de estafas a través de medios cibernéticos e informáticos?	○	○	○	○
¿Considera que las autoridades realizan una labor adecuada para solucionar este delito?	○	○	○	○
¿Considera que los funcionarios de la Dirección de Investigación Judicial (DIJ) y de Criminalística, realizan eficazmente los procedimientos de investigación judicial para solucionar de este delito?	○	○	○	○

Se enviará una copia de tus respuestas por correo electrónico a la dirección que has proporcionado.

Enviar

Borrar formulario

ANEXO N° 3

PERMISOS DE LA INVESTIGACIÓN

UNIVERSIDAD ESPECIALIZADA DE LAS AMÉRICAS
Extensión Universitaria de Coclé
El Jagüito, vía Interamericana. Antón.
"Caminando hacia la Excelencia"
Teléfono: 906-0206 Correo electrónico: extension.cocle@udelas.ac.pa

Antón, 26 de noviembre de 2021
EUC-743-2021

Doctor
José Pachar
Director General
Instituto de Medicina Legal y Ciencias Forenses
E. S. D.

Distinguido Doctor:

Reciba un cordial y atento saludo de parte de la familia udelista, y el deseo de éxitos en sus funciones diarias.

Con la presente deseamos hacer de su conocimiento que el joven **Luis Pérez**, con cédula de identidad personal **2-744-591**, correo electrónico: luis.perez.1@udelas.ac.pa, estudiante graduando de la Licenciatura en Investigación Criminal y Seguridad, ha mostrado interés en desarrollar un trabajo de grado titulado: **Procedimientos en la investigación judicial de estafas a través de medios cibernéticos o informáticos,** con el objetivo de analizar los procedimientos utilizados para la investigación de las estafas a través de medios cibernéticos o informáticos en el corregimiento de Aguadulce, por lo cual solicitamos su permiso para que el estudiante pueda desarrollar la investigación, en la agencia de Coclé, de la institución que usted dirige.

En tal sentido, el estudiante en mención se compromete a cumplir los requisitos que establezca su institución, los lineamientos académicos y éticos que establece nuestra universidad, así como las normas de seguridad sanitaria que se requiere en estos momentos, bajo el seguimiento y asesoría de la profesora Mitzila Acosta Herrera, docente de trabajo de grado, localizable al número de celular 6735-4894.

Agradecemos todo el apoyo y colaboración que su institución pueda ofrecer al estudiante en esta última etapa de su formación universitaria.

Cordialmente,

Doctorando Daivis Guerra Monterrey
Director Extensión Universitaria de Coclé
daivis.guerra@udelas.ac.pa
Cel. 6923-8458

EXTENSIÓN UNIVERSITARIA DE COCLÉ

MINISTERIO PÚBLICO
INSTITUTO DE MEDICINA LEGAL
Y CIENCIAS FORENSES
AGENCIA DE COCLÉ
Recibido por:
Hora: 2:35 p.m.
Fecha: 6-12-2021

UNIVERSIDAD ESPECIALIZADA DE LAS AMÉRICAS
Extensión Universitaria de Coclé
El Jagüito, vía Interamericana. Antón.
"Caminando hacia la Excelencia"
Teléfono: 906-0206 Correo electrónico: extension.cocle@udelas.ac.pa

Antón, 26 de noviembre de 2021
EUC-745-2021

Capitán
Cesar Ortiz
Jefe de la seccional de Investigación Judicial
de Aguadulce
E. S. D.

Respetado Capitán Ortiz:

Reciba un cordial y atento saludo de parte de la familia udelista, y el deseo de éxitos en sus funciones diarias.

Con la presente deseamos hacer de su conocimiento que el joven **Luis Pérez**, con cédula de identidad personal **2-744-591**, estudiante graduando de la Licenciatura en Investigación Criminal y Seguridad, ha mostrado interés en desarrollar un trabajo de grado titulado: **Procedimientos en la investigación judicial de estafas a través de medios cibernéticos o informáticos,** por lo cual solicitamos su permiso para que el estudiante pueda desarrollar la investigación dentro de la institución que usted dirige.

En tal sentido, el estudiante en mención se compromete a cumplir los requisitos que establezca su institución, los lineamientos académicos y éticos que establece nuestra universidad, así como las normas de seguridad sanitaria que se requiere en estos momentos, bajo el seguimiento y asesoría de la profesora Mitzila Acosta Herrera, docente de trabajo de grado.

Agradecemos todo el apoyo y colaboración que su institución pueda ofrecer al estudiante en esta última etapa de su formación universitaria.

Cordialmente,

UDELAS
EXTENSIÓN UNIVERSITARIA DE COCLÉ

Doctorando Daivis Guerra Monterrey
Director Extensión Universitaria de Coclé
daivis.guerra@udelas.ac.pa
Cel. 6923-8458

REPÚBLICA DE PANAMÁ
MINISTERIO PÚBLICO
INSTITUTO DE MEDICINA LEGAL Y CIENCIAS FORENSES
SECRETARÍA DE DOCENCIA, INVESTIGACIÓN Y NORMATIVA
Edificio Albrook Canal Plaza, Telefax 232-8617
secretaria.docenciaimelcf@gmail.com

Panamá, 20 de diciembre de 2021
OFICIO IMELCF-SDIN-218-2021

Doctor
DAIVIS GUERRA MONTERREY
Director
Extensión Universitaria de Coclé
UDELAS

Doctor Guerra:

En atención a su Nota-EUC-743-2021, fechada 26 de noviembre del año en curso, donde detalla el interés del estudiante **Luis Pérez**, con cédula de identidad personal **N° 2-744-591** de la Licenciatura en Investigación Criminal y Seguridad en realizar el trabajo de grado titulado **"Procedimientos en la Investigación Judicial de Estafas a través de medios cibernéticos o informáticos"** , con el objetivo de analizar los procedimientos utilizados para la investigación de las estafas, específicamente en el Corregimiento de Aguadulce, tengo a bien dar la siguiente respuesta:

Hemos hecho las consultas pertinentes a la Subdirección de Criminalística para evaluar la solicitud del estudiante; sin embargo, nos manifiestan que en la Agencia de Coclé no se cuenta con Unidad de Informática Forense, todos los casos en esta provincia son atendidos por la Agencia de Los Santos.

Por lo antes expuesto le comunico que se ha otorgado Visto bueno para que el estudiante realice su trabajo de grado en la Agencia de Criminalística de Los Santos.

Para coordinar la logística correspondiente, favor contactar al Lcdo. Raúl Pereira, Coordinador de la Agencia de Criminalística de Los Santos, al número telefónico: 994-2468 o al correo electrónico: crimlossantos07@gmail.com

Aprovecho la oportunidad para presentarle las seguridades de mi consideración y respeto.

Atentamente,

Doctora
GISELA JURADO IGLESIAS
Secretaria de Docencia, Investigación y Normativa

SECRETARIA DE DOCENCIA
INVESTIGACION Y NORMATIVA

C.I. Dr. José Vicente Pachar Lucio, Director General
Lcdo. Francisco Wellington, Subdirector de Criminalística, encargado
SDIN/Hilda

INDICE DE CUADROS

ÍNDICE DE TABLAS

ÍNDICE DE IMÁGENES

ÍNDICE DE GRÁFICAS