REPUBLICA BOLIVARIANA DE VENEZUELA

UNIVERSIDAD JOSE ANTONIO PAEZ

FACULTAD DE CIENCIAS JURIDICAS Y POLITICAS

Análisis de la eficiencia del régimen probatorio venezolano con respecto al manejo de evidencias digitales y las experticias cibernéticas en la materia Penal

Alumno:

Víctor Velasco

V-27.657.553

Tutor Institucional:

Prof. Teresa Méndez

V- 5.061.814

San Diego, 11 de octubre de 2022

UNIVERSIDAD JOSÉ ANTONIO PÁEZ
FACULTAD DE CIENCIAS JURÍDICAS Y POLÍTICAS
ESCUELA DE DERECHO
COORDINACIÓN DE PASANTÍA Y TRABAJO DE GRADO

ACTA DE APROBACIÓN

INFORME FINAL DE PASANTÍA ☐

TRABAJO DE GRADO [X]

El jurado designado por la Facultad de Ciencias Jurídicas y Políticas para la evaluación del Informe Final de Pasantía o Trabajo de Grado titulado: Análisis de la eficiencia del régimen probatorio venezolano con respecto al manejo de evidencias digitales y las experticias cibernéticas en la materia Penal.

Realizado por (el) (la) Br: Víctor David Velasco Ferrer, C.I. N°: 27. 657.553 cursante de la carrera de Derecho, hace constar después de analizar su contenido y oída la exposición oral, considera que el informe final o Trabajo de Grado ha obtenido la calificación de: VEINTE PUNTOS

APROBADO [X] NO APROBADO ☐

El Jurado

Tutor Académico
Apellido/Nombre:
Teresa Méndez
C.I: 5.061.814

Jurado
Apellido/Nombre:
C.I: 6402557

Jurado
MARINA SILVA
Apellido/Nombre:
C.I: 7332513

Fecha: 14/10/22

Resumen

REPUBLICA BOLIVARIANA DE VENEZUELA

UNIVERSIDAD JOSE ANTONIO PAEZ

FACULTAD DE CIENCIAS JURIDICAS Y POLITICAS

Análisis de la eficiencia del régimen probatorio venezolano con respecto al manejo de evidencias digitales y las experticias cibernéticas en la materia Penal

Alumno: Víctor Velasco

C.I: 27. 657.553

Tutor Institucional: Prof. Teresa Méndez

V- 5.061.814

El presente trabajo investigativo tiene como objetivo, comprender las líneas generales el estado, técnico y jurídico del Régimen probatorio venezolano con respecto a evidencias digitales y experticias cibernéticas, partiendo de un análisis al marco metodológico, para el tratamiento de evidencia que establece nuestro Código Procesal Penal, es decir, el Manual Único de Cadena de Custodia. A su vez, esta investigación procura concientizar e ilustrar a los investigadores penales y profesionales del Derecho que se desempeñan dentro de la administración pública o el ejercicio privado, acerca de la importancia del manejo idóneo de la evidencia digital, como medio probatorio fundamental para el esclarecimiento de hechos ilícitos en materia informática.

Palabras Clave: Derecho Penal, Informática Forense, Investigación Penal, Régimen Probatorio, Pruebas, Evidencia, Evidencia Digital, Experticias.

Línea de Investigación: Sistema Penal y Administración de Justicia.

Agradecimientos

Primeramente, le agradezco a Dios por permitirme la sabiduría para realizar este trabajo de investigación, a su vez por permitirme completar este objetivo de mi formación académica.

En segundo a lugar, a mis padres por el esfuerzo económico realizado.

En tercer lugar y aunque peque de tener alta autoestima, quiero agradecerme a mí mismo, por el esfuerzo colocado cada semestre, me agradezco por los desvelos soportados y por los momentos frustrantes sorteados. A su vez agradezco a aquellos compañeros que me acompañaron desde el día uno, son pocos los que podrán completar este objetivo en conjunto con mi persona, lamentablemente las adversidades de la pandemia confabularon en su contra, pero solo ellos saben el esfuerzo que día a día realizamos los estudiantes, lo que luchamos por llegar a la meta, espero que pronto les llegue su merecido momento.

Finalmente, a mi tutora, la Prof. Teresa Méndez por su paciencia y su oportuna asesoría durante el desarrollo del presente trabajo investigativo.

Dicho esto, me despido con la esperanza de que el presente trabajo investigativo sea académica e intelectualmente nutritivo.

ÍNDICE

Introducción

Durante la década de los 80s inició un apogeo tecnológico con consecuencias y beneficios en todos los niveles de la vida humana, las nuevas tecnologías constituyeron un avance para la optimización de las actividades productivas para el colectivo, destacando inicialmente, en el ámbito Financiero, industrial y las telecomunicaciones. Sin embargo, este avance progresivo del componente tecnológico en la vida cotidiana, también supuso el nacimiento de una serie de conductas y actividades relacionadas al uso de la tecnología, que no se encontraban reguladas por el ordenamiento jurídico.

En este orden de ideas, es menester resaltar que también se ampliaron las fronteras del Delito, los delincuentes empezaron a valerse de los medios tecnológicos para optimizar las prácticas delictivas clásicas y a su vez empezaron a desarrollar novedosas prácticas delictivas relacionadas directamente al uso delictivo de la tecnología, podemos afirmar esto debido a que precisamente durante esa década se registraron los Primeros delitos perpetrados a través de medios informáticos. Para darle mayor basamento a dicha afirmación podemos citar casos como el de Ian Murphy, en el año 1981, considerado como la primera persona en ser condenada por un delito cibernético, el delincuente anteriormente nombrado hackeó la red de la compañía de telecomunicaciones AT&T y cambió el reloj interno para recargar tarifas fuera del horario, la aparición de este tipo de casos ocasionó que en el año 1986 el congreso de los Estados Unidos de Norte América promulgará la Ley de Fraude y Abuso de Computadoras.

Posteriormente en la década comprendida entre el año 2000 y el año 2010, existieron múltiples casos de fraudes y delitos con carácter informáticos, que obligaron a las naciones del mundo a legislar para poder sancionar efectivamente a dichos delitos, entre ellas, la República Bolivariana de Venezuela la cual promulgó la Ley especial contra los Delitos Informáticos en 30 de octubre de 2001, una ley bastante corta y pero que sirvió de marco normativo para sancionar dichas acciones. Cabe destacar que los delitos comunes no son las únicas actividades ilícitas que pueden realizarse a través de medios digitales, así como los delincuentes comunes desarrollaron nuevas técnicas para perpetrar delitos, las células terroristas, desarrollaron el Ciberterrorismo, una actividad que se vale de los medios digitales para la desestabilización, ya sea mediante ataques a redes gubernamentales, robo de información gubernamental o la difusión masiva de materia multimedia que infunda terror.

A su vez los delitos y el sabotaje cibernético se han convertido en un arma para la desestabilización de Países, aplicada por aquellos gobiernos que pretenden de manera criminal hacer daño a sus adversarios políticos como ejemplo podemos tomar el Ataque a la red eléctrica de Ucrania efectuado en diciembre del año 2015, ocasionando que 230.000 personas aproximadamente, quedaran sin energía durante 6 horas, este ataque dejo un precedente histórico pues se cree que este ataque fue el primero en afectar con éxito una red de distribución de electricidad. Dicho ataque afectó tres regiones de Ucrania, el servicio de seguridad ucraniano culpó al Gobierno ruso por el ataque, acusación que posteriormente seria confirmado por una serie de compañías privadas de seguridad de Estados Unidos que investigaron el suceso.

Este tipo de hechos delictivos también se suscitan en la República para mayor ejemplificación citamos lo acontecido el 27 de junio del presente año 2022. Cuando un grupo de hackers logró vulnerar la seguridad informática del Ministerio del Poder Popular para la Defensa, logrando filtrar más de 5.000 mil archivos confidenciales de la Junta Permanente de Evaluación de la Armada Bolivariana, los piratas informáticos, conocidos con el nombre Team HDP, accedieron a información privilegiada sobre Guardias de Honor, DGCIM, SEBIN, Funcionaros de alto perfil e incluso espías en otros países. Los hechos anteriormente enunciados en estos párrafos introductorios, serán estudiados en el presente trabajo investigativo, centrándonos específicamente en el componente probatorio necesario para judicializar estas acciones y así lograr combatir tanto la delincuencia común que se vale de los medios informáticos para optimizar la comisión de actividades ilícitas, como la delincuencia informática directamente.

Capítulo I: Planteamiento del Problema

Actualmente en la República Bolivariana de Venezuela los delincuentes se valen de los medios tecnológicos para perpetrar delitos comunes tipificados por el Código Penal venezolano, como la extorsión y el fraude, pero a su vez se valen de los mismos para realizar delitos consagrados en la Ley especial contra los Delitos Informáticos. En ese orden de ideas es necesario desarrollar un marco metodológico adecuado para el manejo de la evidencia obtenida en el sitio donde se suscitó el hecho delictivo, el presente trabajo investigativo está orientado al estudio de dichos delitos, específicamente, al material probatorio utilizado para la judicialización de los mismos, abarcando todo lo relativo al régimen probatorio con respecto a las evidencias digitales, iniciando por su correcta obtención, su proceso de resguardo y hasta su admisión como prueba para ser valorada por el Juez competente.

El régimen probatorio venezolano en materia penal permite a las partes valerse de cualquier elemento de convicción que cumpla con los requisitos de legalidad, licitud, idoneidad y utilidad de la prueba. La prueba constituye la piedra angular de la resolución de las controversias jurídicas y en este caso, para el esclarecimiento de hechos punibles. En nuestro país, los medios de prueba se encuentran diseñados para recolectar evidencia física y no evidencia digital, esta última incorpora al proceso penal a través del principio de libertad probatoria.

Las evidencias digitales y las experticias cibernéticas constituyen el elemento de convicción más importante para la persecución de delitos informáticos. Mediante las misma los funcionarios competentes y el juez podrán dar respuesta a las responder este procedimiento se pretende responder a las preguntas de oro de la investigación Penal: **¿qué?, ¿quién?, ¿dónde?, ¿cuándo?,**

¿por qué?, ¿con que? Y ¿cómo? Es redundante seguir explicando la gran importancia que están asumiendo los medios probatorios informáticos en los últimos años, ya que cada día es más habitual tener que hacer frente a diferentes incidentes relacionados con la seguridad informática. La obtención, el resguardo y la apreciación adecuada de las pruebas digitales permite garantizar la Judicialización de delitos como:

- **Fraude Informático**

Este delito se presenta cuando una persona o un grupo de personas se vale de artificios o cualquier medio capaz de engañar o sorprender la buena fe de otro, induciéndole en error, procurando para sí o para otros un provecho injusto con perjuicio ajeno. Como se ha indicado con anterioridad, los avances tecnológicos también pueden utilizarse para perpetrar delitos en este apartado podemos enunciar actividades delictivas como las estafas con criptoactivos o las estafas telefónicas.

- **Robo de Propiedad Intelectual**

La Organización Mundial de la Propiedad Intelectual (OMPI) define la propiedad intelectual como **"los derechos sobre las creaciones de la mente, tales como las invenciones, las obras literarias y artísticas, los diseños y los símbolos, nombres e imágenes utilizados en el comercio".**

El Robo de Propiedad Intelectual consiste en el acceso, distribución o uso de la propiedad intelectual, sin la autorización inicial del propietario o los propietarios de esta, violentando el bien jurídico que la misma constituye. La Propiedad Intelectual se encuentra ubicada dentro de la esfera de los Derechos de Propiedad, aunque no coincida con el concepto común de Robo (en el cual se

priva al sujeto pasivo de la propiedad física), en el Robo de Propiedad Intelectual se le niega es el control, la gestión y el beneficio económico que debe derivarse del uso posterior de su propiedad intelectual. Como ejemplo informático de este tipo de delitos podemos citar la Piratería informática, que consiste en la distribución gratuita de contenido que legalmente debería de consistir en una remuneración para su autor.

- **Falsificación de Documentos**

Este delito ocurre cuando se alteran datos de los documentos almacenados, este caso de forma computarizada. Los dispositivos electrónicos pueden utilizarse también para efectuar falsificaciones de documentos, de tal calidad que sólo un software especializado o un experto puede diferenciarlos de los documentos auténticos.

- **Sabotaje Informático**

Es el acto de borrar, suprimir o modificar sin autorización funciones o datos de computadora con intención de obstaculizar el funcionamiento normal del sistema. Las principales técnicas que permiten cometer sabotajes informáticos son:

a) ***Bombas Lógicas (Logic Bombs):*** es una especie de bomba de tiempo que debe producir daños posteriormente. Exige conocimientos especializados ya que requiere la programación de la

destrucción o modificación de datos en un momento dado del futuro. Ahora bien, al revés de los virus o los gusanos, las bombas lógicas son difíciles de detectar antes de que exploten; por eso, de todos los dispositivos informáticos criminales, las bombas lógicas son las que poseen el máximo potencial de daño. Su detonación puede programarse para que cause el máximo de daño y para que tenga lugar mucho tiempo después de que se haya marchado el delincuente. La bomba lógica puede utilizarse también como instrumento de extorsión y se puede pedir un rescate a cambio de dar a conocer el lugar en donde se halla la bomba.

b) ***Gusanos:*** Se fábrica de forma análoga al virus con miras a infiltrarlo en programas legítimos de procesamiento de datos o para modificar o destruir los datos, pero es diferente del virus porque no puede regenerarse. En términos médicos podría decirse que un gusano es un tumor benigno, mientras que el virus es un tumor maligno. Ahora bien, las consecuencias del ataque de un gusano pueden ser tan graves como las del ataque de un virus: por ejemplo, un programa gusano que subsiguientemente se destruirá puede dar instrucciones a un sistema informático de un banco para que transfiera continuamente dinero a una cuenta ilícita.

- **Pornografía infantil**

En líneas generales, la elaboración, difusión y comercialización de contenido pornográfico constituyen hechos punibles sancionables por el ordenamiento jurídico venezolano. Sin embargo, el legislador venezolano otorga un castigo mucho mas severo cuando se trata de contenido explícito en el cual esté presente la utilización de niños, niñas y adolescentes. En este orden de ideas es menester indicar que las actividades anteriormente enunciadas constituyen una problemática a

nivel mundial y existen grupos delictivos de dedicados exclusivamente a la distribución y comercialización de este tipo de contenido.

- **Espionaje Informático y el hurto de información**

El espionaje informático supone tanto acceder, como conocer indebidamente los datos en un sistema informático. A continuación, enunciaremos las modalidades mas comunes de Espionaje informático y el hurto de información, no quiere decir que sean los únicos, también existen los Spyware, es decir, software especializados en el espionaje.

a) ***Fuga de datos (Data Leakage):*** también conocida como la divulgación no autorizada de datos reservados, es una variedad del espionaje industrial que sustrae información confidencial de una empresa. A decir de Luis Camacho Loza, "la facilidad de existente para efectuar una copia de un fichero mecanizado es tal magnitud en rapidez y simplicidad que es una forma de delito prácticamente al alcance de cualquiera"38. La forma más sencilla de proteger la información confidencial es la criptografía.

b) ***Reproducción no autorizada de programas informáticos de protección legal:*** Esta puede entrañar una pérdida económica sustancial para los propietarios legítimos. Algunas jurisdicciones han tipificado como delito esta clase de actividad y la han sometido a sanciones penales. El problema ha alcanzado dimensiones transnacionales con el tráfico de esas reproducciones no autorizadas a través de las redes de telecomunicaciones modernas. Al respecto, considero, que la reproducción no autorizada de programas informáticos no es un

delito informático, debido a que, en primer lugar el bien jurídico protegido es en este caso el derecho de autor, la propiedad intelectual y en segundo lugar que la protección al software es uno de los contenidos específicos del Derecho informático al igual que los delitos informáticos, por tal razón considero que la piratería informática debe ser incluida dentro de la protección penal al software y no estar incluida dentro de las conductas que componen la delincuencia informática.

- **Sniffing (Uso de Sniffer).**

Un sniffer consiste en una herramienta de software o hardware que permite al usuario supervisar su tráfico en Internet y capturar todo el tráfico de datos que entran y salen de su equipo, en tiempo real. En este orden de ideas, el Sniffing es el uso de la herramienta anteriormente nombrada, el cual por si solo no es una actividad delictiva, sin embargo, como veremos más adelante puede ser constituir un medio para la comisión de hechos punibles. En este orden de ideas es necesario indicar que existen dos tipos de Sniffing: **Activo y Pasivo.**

a) ***Sniffing Activo:*** A medida que conecta más dispositivos a un concentrador, el nivel de tráfico puede llegar a ser abrumador. Los conmutadores de red son la solución a este problema. Los conmutadores regulan el tráfico de la red enviando los datos al dispositivo al que están destinados. Un sniffer pasivo en un concentrador de red solo podrá ver los datos que entren y salgan de esa máquina. Aquí es donde entra el juego el sniffing activo. Para acceder a todo el tráfico que circula a través de la red, un sniffer activo debe superar la forma de direccionamiento de los conmutadores. Existen varias formas de conseguirlo, pero todas ellas implican inyectar

tráfico adicional en la red. Esto es lo que lo convierte en un proceso activo y lo diferencia de la forma pasiva. La ventaja para sus posibles víctimas está en que es más fácil de detectar, porque delata su presencia.

a) ***Sniffing Pasivo:*** Los concentradores son simples dispositivos de red que interconectan varios dispositivos en una sola red. No existen mecanismos reguladores que dirijan el tráfico a su destinatario; en lugar de ello, todos los dispositivos reciben todo el tráfico y luego determinan si ese tráfico es relevante o no. Como todos los dispositivos del concentrador reciben todo el tráfico de la red, el sniffer puede absorber fácilmente, y de forma pasiva, todo lo que se envía. No hay nada que *hacer* más que sentarse a esperar. Esto hace que el sniffing pasivo sea muy difícil de detectar. No imposible, pero sí difícil.

Los ciberdelincuentes pueden pinchar una red para ver todo el tráfico que se envía a través de la misma. Al supervisar el uso de Internet, incluyendo los correos electrónicos y los mensajes instantáneos, un hacker podría acceder a las credenciales de inicio de sesión, información privilegiada y datos financieros. Por eso los sniffers son tan peligrosos en manos equivocadas. Y hay muchos sniffers gratuitos disponibles en línea: música celestial para los oídos de un ciberdelincuente.

- **Phishing**

El Phishing es una técnica que consiste en el envío de un correo electrónico en el que los ciberdelincuentes suplantan la identidad de entidades, como nuestro banco, una red social, una entidad pública, una empresa reconocida o un servicio que utilicemos, y su objetivo es obtener toda

la información personal y bancaria que puedan conseguir de nosotros, como usuarios y contraseñas, direcciones, datos de tarjetas de crédito, etc., realizar un cargo económico o infectar el dispositivo. Para ello, adjuntan archivos infectados o enlaces a páginas fraudulentas.

- **Deepfake**

Los Deepfakes son archivos multimedia manipulados mediante un software de inteligencia artificial de modo que parezcan originales, auténticos y reales. Dichos archivos son generados haciendo uso de softwares de inteligencia especializados en aprendizaje profundo y automático que copilan contenido multimedia, obteniendo la capacidad de falsificar el contenido de imágenes, videos y sonidos, procurando una aparente autenticidad que en ocasiones solo puede ser impugnada mediante programas informáticos especializados.

Al igual que el Sniffing, el uso de Software para la creación de Material manipulado a partir de tecnología de Deepfake, no constituye por sí solo un hecho delictivo. Por ejemplo, se puede hacer uso de un Deepfake para calumniar a la administración de Justicia utilizando pruebas digitales contaminadas o manipuladas, por eso es necesario comprender que los Órganos de Investigación Penal y Criminalística deben adecuarse para combatir el uso delictivo de este tipo de Software.

- **Ciberterrorismo**

Para poder comprender plenamente este hecho delictivo, es necesario desarrollar una serie de definiciones previas. En primer lugar debemos entender que se entiende dentro de nuestro ordenamiento Jurídico por Terrorismo o Actos Terroristas, estos constituyen una serie de acciones

delictivas desarrollados dolosamente por un grupo de personas o individualmente, que por su naturaleza puedan perjudicar gravemente a un País o a una Organización Internacional, ya sea con la finalidad de intimidar a una población, obligar indebidamente a los gobiernos o a una organización internacional a realizar un acto o a abstenerse de hacerlo. En líneas generales, actos realizados con la intención de desestabilizar gravemente o destruir las estructuras políticas, económicas o sociales de un país o de una organización internacional. Como se ha indicado desde el primer título del presente trabajo de investigación, es posible perfeccionar delitos a partir del uso de equipos informáticos y digitales, esto quiere decir que la gama de actividades delictivas se amplió con el uso de la tecnología. Así nació lo que en la actualidad conocemos como Ciberterrorismo, una actividad adjunta al Terrorismo, que se basa en el uso de la tecnología para la desestabilización de naciones y organizaciones Internacionales.

Formulación del Problema

¿Cuál es la metodología aplicada actualmente por los organismos policiales y de investigación penal para garantizar la integridad de las evidencias de carácter digital y cibernético**?**

¿Existe en el Manual único de Cadena de custodia una serie de procedimientos estandarizados que garanticen el manejo adecuado de la evidencia digital?

¿Son conscientes los funcionarios integrantes del Poder Judicial y en líneas generales los profesionales del derecho, acerca del valor probatorio de las Pruebas Digitales?

Objetivos de la Investigación

Objetivo General

Determinar cuál es el estatus actual del Régimen Probatorio venezolano, a la hora de tratar con evidencia obtenida a partir de medios digitales y cibernéticos, que luego del proceso técnico-jurídico que establece nuestro Código Procesal Penal pasaran a constituir material probatorio.

Objetivos específicos

- Identificar la metodología aplicada actualmente por los organismos policiales y de investigación penal para garantizar la integridad de las evidencias de carácter digital y su idoneidad.

- Precisar si existe en el Manual único de Cadena de custodia vigente, una serie de procedimientos estandarizados que garanticen el manejo adecuado de la evidencia digital.

- Concientizar acerca del valor Probatorio de las evidencias Digitales en el Proceso Penal Venezolano para el esclarecimiento y Judicialización de hechos punibles.

Justificación de la Investigación

El Presente proyecto de investigación tiene por finalidad desentrañar el estado actual del Régimen Probatorio venezolano con respecto al manejo de la evidencia de carácter digital y las experticias cibernéticas, por lo tanto constituye un análisis que nos permitirá determinar si los medios de obtención y el procedimiento de Resguardo aplicados actualmente, son los idóneos para garantizar la integridad de las evidencias precitadas, hasta el inicio de Procedimiento de la Evacuación de Pruebas y su posterior apreciación por parte del Juez competente en Materia Penal.

En líneas generales la justificación del presente trabajo de investigativo, está basada en la concientización ante la posible falta de capacitación, herramientas óptimas, legislación y desarrollo de procedimientos adecuados que regulen la actuación de los organismos dedicados el ejercicio del servicio Policial, investigación penal y criminalística, del Ministerio público o cualquier otra persona que por razones de sus competencias mantenga contacto con elementos que puedan constituir evidencias de carácter digital o cibernético. Y así prevenir practicas deficientes durante la obtención, peritaje y resguardo de evidencia digital, que puede constituir material probatorio de suma importancia para el esclarecimiento de hechos punibles, con la intención de garantizar la Justicia que constituye uno de los fines principales del estado y un valor fundamental del accionar de la República y su ordenamiento jurídico.

Alcance de la Investigación

- La presente investigación tiene como fin, comprender las líneas generales el estado, técnico y jurídico del Régimen probatorio venezolano con respecto a evidencias digitales y cibernéticas.

- Esta investigación procura ilustrar a los investigadores penales y profesionales del Derecho que se desempeñan dentro de la administración pública o el ejercicio privado dentro del espacio territorial de la República Bolivariana de Venezuela, acerca de la importancia del manejo idóneo de la evidencia digital.

- A su vez esta investigación promueve el desarrollo de un marco metodológico para la obtención técnica y el peritaje de evidencia digital.

Limitación de la investigación

- La descuidada y desactualizada legislación a nivel nacional con respecto a la materia.

- La falta de guías técnicas relativas a la metodología aplicable a la obtención de evidencia digital y cibernética, dirigidas a los investigadores nacionales. Por consiguiente, el contenido teórico y académico debe abstraerse de contenido desarrollado en otros países.

- El periodo para la compilación de información y el desarrollo del presente trabajo comprende desde el mes de julio al mes de octubre del año en curso.

Capítulo II: Marco Teórico

Los antecedentes teóricos que inspiraron el presente trabajo investigativo tienen origen internacional, sin embargo, también está presente material académico de origen nacional.

Antecedentes teóricos

- **Efectividad de la Prueba electrónica en el Proceso Penal venezolano mediante su valoración en la administración de justicia (2013). Carabobo, Venezuela. Universidad de Carabobo**. Autor: Martha Emilia Padrón Prado, para optar al grado de "**Especialista en Derecho Penal".**

Esta investigación tuvo como objetivo general determinar la efectividad de la Prueba Electrónica mediante su Valoración en la Administración de Justicia en el Proceso Penal. Se justifica en el hecho que la prueba electrónica, constituye un importante elemento de convicción que funciona mediante la tecnología de información.

Dicha investigación tiene su basamento teórico en la Teoría. del Bien jurídico, la Teoría Tradicional y la Teoría Moderna. Se constituye como una investigación documental y de campo, de tipo descriptivo; la población y muestra estará constituida por 36 sujetos que laboran en el Circuito Jucicial Penal del Estado Carabobo, a quienes se les aplicó un instrumento tipo encuesta en su modalidad de cuestionario con preguntas cerradas, el cual se sometió al juicio de expertos, quienes constataron la coherencia de los objetivos propuestos en la investigación y los ítemes formulados.

Para determinar su confiabilidad, se utilizó la Ecuación de Kuder-Richarsdson (Kr-20). Se concluye que el camino recorrido por el derecho ha sido importante pero insuficiente para los cambios que se vienen en esta era digital, puesto que las apariciones de nuevas tecnologías incrementan la necesidad de modificar la estructura del Derecho en una sociedad, por tanto la tendencia del ordenamiento jurídico ha de ser la de recoger las normas que los propios actores de los medios electrónicos utilizan y darles validez jurídica.

- **Mecanismos de Control y Contradicción de los documentos electrónicos como medios de prueba en el Proceso Penal venezolano (2013). Trujillo, Venezuela. Universidad Católica Andrés Bello. Autor:** Abg. Rafael Echeto, para optar al Título **"Especialista en Ciencias Penales y Criminológicas".**

El objetivo general de esta investigación se centra en establecer los mecanismos de control y contradicción de los documentos electrónicos como medios de prueba en el proceso penal venezolano y el código Orgánico Procesal Penal (2012), junto a la Constitución de la República Bolivariana de Venezuela (1999), rigen con respecto a los documentos como medios probatorios y el respeto al debido proceso que posee cada ciudadano. Asimismo, la metodología empleada en este trabajo fue de tipo documental, fundamentada de modo bibliográfico, en donde se emplearon prácticas de búsqueda de información y se hicieron los análisis correspondientes.

La Investigación precitada nos permitió obtener nociones básicas relativas a los medios para el control de la documentación electrónica, apartado que sumamente importante para nuestra investigación pues los documentos electrónicos constituyen una buena parte de lo que procesalmente se entiende por pruebas electrónicas, lo cual lógicamente es objeto de estudio en el presente trabajo.

- **La Obtención de pruebas en delitos cibernéticos en las Fiscalías Especializadas en Ciberdelincuencia de Lima Centro (2021). Callao, Perú. Universidad Cesar Vallejo**. **Autores:** Hernández Ayala, Nancy y Patricio Rojas, Alejandro Efraín, para optar al título profesional de **"Abogado".**

La investigación precitada tuvo como objetivo analizar la afectación de la actuación fiscal en la obtención de pruebas digitales en la Fiscalía Corporativa Especializada en Ciberdelincuencia de Lima – Centro en el año 2021. La población estuvo conformada por los fiscales y asistentes de la Fiscalía Especializada en Ciberdelincuencia de Lima Centro. La técnica utilizada fue la entrevista y el instrumento fue guía de entrevista. Se concluyó que, debido a la falta de capacitación, herramientas óptimas y la legislación, la actuación fiscal es deficiente en la obtención y peritación de evidencia digital, información importante, para el planteamiento de la teoría del caso en las investigaciones seguidas contra los delitos de fraude informático y suplantación de identidad, lo que genera, una insuficiente protección de los bienes jurídicos tutelados.

Finalmente, se recomienda la implementación de más Fiscalías Especializadas en Ciberdelincuencia en todo el país, implementación de herramientas que ayuden con el acopio de la evidencia digital, una mayor especialización y capacitación a las Instituciones que se ven involucradas en la lucha contra los delitos cibernéticos, políticas de prevención por parte del Estado y la creación de un protocolo de peritación de evidencia digital.

En líneas generales esta investigación, nos sirvió para darle un mejor enfoque a uno de los objetivos planteados en la presente investigación, específicamente: Analizar si la metodología aplicada actualmente por los organismos policiales y de investigación penal, es la idónea para garantizar la integridad de las evidencias de carácter digital y cibernético.

- **Evidencia informática: ¿Un nuevo paradigma para el derecho procesal penal? (30 de junio de 2021). Buenos Aires, Argentina. Universidad de San Andrés.** Autora: Natalia Schirakian, para optar al grado de **"Especialista en Derecho Penal".**

En los Códigos Procesales Penales de la hermana República Argentina, en general, no se encuentran previstos los medios de prueba específicos para poder incorporar la evidencia digital a las investigaciones penales. Ante la falta de regulación, los operadores del sistema judicial se han visto obligados a incorporar este tipo de evidencia a través del principio de "libertad probatoria", utilizando la analogía como herramienta principal. Este escenario trajo consigo significativos problemas, toda vez que se vieron vulnerados derechos y garantías de los ciudadanos.

Tomando en consideración los eventos ocurridos en la hermana república, hicimos uso del trabajo investigativo de la Abog. Natalia Schirakian para obtener una mayor compresión de la problemática, con la finalidad de promover la adecuación del Régimen probatorio venezolano y así prevenir la manifestación de sucesos que atenten contra el debido proceso.

- **La Evidencia Digital y los Delitos Informáticos en el Sistema Jurídico Peruano (febrero, 2022). Lima, Perú. Universidad Peruana de las Américas. Autor:** Gallegos Osorio, Sigfredo Antonio, para optar al Título Profesional de **"Abogado".**

A raíz de los constantes avances en la información, tecnología y en el mundo de las comunicaciones, nos debemos dar cuenta cómo la tecnología influye en nuestras vidas y acciones día a día. El trabajo precitado presenta las condiciones que se deben tomar en cuenta en la revisión

de las pruebas digitales y cómo se deben utilizar en los procedimientos judiciales, Así como, lo relacionado al cibercrimen, la Convención de Budapest, los criterios internacionales y nacionales referentes a este tema. También, las pruebas obtenidas y las evidencias digitales en el proceso. El perfil del ciberdelincuente ha cambiado notoriamente, antes era aquel sujeto perito en computadoras que se inmiscuía en aspectos confidenciales y en la mayoría de los casos los fines siempre son económicos. La investigación se enfocará en los delitos cibernéticos y las medidas tomadas de parte del Estado peruano y de la regulación de otros países.

Bases Teóricas

Evidencia Digital

La evidencia digital, es todo aquel dato informático avanzado o dispositivo con carácter digital o electrónico que pueda ser de utilidad para el esclarecimiento de hechos punibles o que luego del procedimiento técnico-jurídico correspondiente pueda constituir material probatorio para la resolución de una controversia jurídica.

Puede ser clasificada de la siguiente manera:

- **Evidencia física con carácter digital o informático:** hace referencia al material informático como, por ejemplo: discos duros, pendrives, teléfonos inteligentes, etc.

- **Evidencia directamente digital:** corresponde a la información almacenada en las evidencias electrónicas. Algunos ejemplos de evidencias digitales son: Correos Electrónicos, Documentos Digitalizados, Firmas Digitales, Fichero en disco, Proceso en ejecución, Log, Archivos temporales, Entradas de registro, etc.

A su vez la Evidencia directamente digital puede sub clasificarse en dos apartados según su naturaleza: **Evidencia Volátil y Evidencia No volátil.**

- **Volátil:** hace referencia a información temporal, como la que reside en la memoria principal (RAM).
- **No volátil:** hace referencia a memoria permanente, es decir, información que se mantiene cuando se apaga el equipo, por ejemplo, datos almacenados en la memoria interna.

Características de la Evidencia Digital

En líneas generales, las evidencias digitales deben contener las siguientes características:

- **Admisible:** debe tener valor legal.
- **Auténtica:** debe ser verídica y no haber sufrido manipulación alguna. Para ello, deben haberse sacado los correspondientes hashes con el fin de asegurar la integridad.
- **Completa:** debe representar la prueba desde un punto de vista objetivo y técnico, sin valoraciones personales, ni prejuicios.
- **Creíble:** debe ser comprensible.
- **Confiable:** las técnicas utilizadas para la obtención de la evidencia no deben generar ninguna duda sobre su veracidad y autenticidad.

Análisis Forense Digital

El análisis forense digital consiste en un conjunto de procedimientos de recopilación y análisis de evidencias que se realizan con el fin de esclarecer ilícitos relacionados con la seguridad informática o corroborar el uso de dispositivos con carácter digital o electrónico en la comisión de hechos punibles, que sirven como pruebas ante un tribunal.

Principio de Locard

A la hora de realizar un análisis forense digital es fundamental tener presente el Principio de intercambio de Locard, unos de los principios fundamentales de la criminalística y el análisis forense en líneas generales, dicho principio indica lo siguiente: **"siempre que dos objetos entran en contacto transfieren parte del material que incorporan al otro objeto".** Esto significa que, en cualquier tipo de delito, incluidos los delitos informáticos, el accionar de un agente irregular deja un rastro, que puede ser identificado mediante el proceso de análisis forense, esto quiere decir, que es posible la obtención de evidencias. Lógicamente, también se cumple el principio de Locard a la hora de realizar el propio análisis forense, por lo tanto, el experto, técnico o perito debe ser sumamente cuidadoso en su accionar para que el sistema se vea afectado en la menor medida posible y evitar la contaminación de las evidencias adquiridas.

Tipos de análisis forense

En líneas generales, el proceso de peritaje de evidencia digital se clasifica tomando en consideración el objeto a analizar, en este orden de ideas podemos afirmar que existen los siguientes tipos de análisis:

1. **Computación forense:** Esta expresión podría interpretarse de dos maneras:

- Como la disciplina de las ciencias forenses, procura descubrir e interpretar la información en los medios informáticos para establecer los hechos y formular las hipótesis relacionadas con el caso.

- Como la disciplina científica y especializada que entendiendo los elementos propios de las tecnologías de los equipos de computación ofrece un análisis de la información residente en dichos equipos.

Estas dos definiciones no son excluyentes, sino complementarias.

2. **Análisis forense de redes:** Este tipo de análisis permite comprender la manera en la cual los protocolos, configuraciones e infraestructuras de comunicaciones se conjugan para dar como resultado un momento específico en el tiempo y un comportamiento particular. Debe ser practicado por un profesional que, entendiendo las operaciones de las redes de computadores, es capaz, siguiendo los protocolos y formación criminalística, de establecer los rastros, los movimientos y acciones que un delincuente ha desarrollado para concluir su acción. A diferencia de la definición de computación forense, este contexto exige capacidad de

correlación de evento, muchas veces disyuntos y aleatorios, que, en equipos particulares, es poco frecuente.

3. **Análisis forense digital:** Este tipo de análisis conjuga de manera amplia todo el apartado digital. Podríamos hacer semejanza con informática forense, al ser una forma de aplicar los conceptos, estrategias y procedimientos de la criminalística tradicional a los medios informáticos especializados o como una disciplina especializada que procura el esclarecimiento de los hechos que podrían catalogarse como incidentes, fraudes o usos indebidos bien sea en el contexto de la justicia especializada o como apoyo a las acciones internas de las organizaciones en el contexto de la administración de la inseguridad informática.

Características

El procedimiento de análisis forense debe poseer las siguientes características:

- **Verificable:** se debe poder comprobar la veracidad de las conclusiones extraídas a partir de la realización del análisis.
- **Reproducible:** se deben poder reproducir en todo momento las pruebas realizadas durante el proceso.
- **Documentado:** todo el proceso debe estar correctamente documentado y debe realizarse de manera comprensible y detallada.
- **Independiente:** las conclusiones obtenidas deben ser las mismas, independientemente de la persona que realice el proceso y de la metodología utilizada.

Fases

El procedimiento de análisis forense consta de las siguientes fases:

- **Preservación:** corresponde a la fase en la que se debe garantizar que no se pierdan las evidencias que deben ser recopiladas para su posterior análisis. El desconocimiento puede provocar que se pierda información relevante y que podría resultar decisiva para la resolución del incidente.

- **Adquisición:** Esta es la etapa en la que se colectan las evidencias.

- **Análisis:** Es la fase en la cual, será la peritación real de la evidencia en Laboratorio.

- **Documentación:** un aspecto fundamental en el proceso del análisis forense es el de la documentación por lo que se debe realizar dicha fase de una manera muy metódica y detallada. Se pueden realizar, entre otras, las siguientes acciones: Fotografiar las pruebas. Cadena de custodia. Documentar todos y cada uno de los pasos realizados durante el proceso, manteniendo una bitácora con fechas y horas de cada acción realizada sobre las evidencias.

- **Presentación:** Es la fase donde se exponen las conclusiones que se han obtenido del proceso del análisis forense. Para ello, es recomendable preparar una presentación de manera pedagógica para que sea fácilmente comprensible y elaborar las conclusiones desde un punto de vista objetivo, sin presentar juicios de valor innecesarios.

Hay que tener presente que las fases no son secuenciales, sino que están entrelazadas entre sí. Por ejemplo, la fase de documentación comienza en la fase de preservación.cc

Metodologías Estandarizadas para la colección y preservación de la Evidencia Digital

Procedimiento para la Adquisición y Resguardo de Evidencia Física con Carácter informático o digital

Procedimientos Asociados al Proceso de Protección

En líneas generales, este tipo de evidencia debe protegerse contra golpes, manipulaciones incorrectas, factores ambientales extremos y de campos magnéticos. Así mismo deben evitarse a toda costa las siguientes conductas:

- No se deberán iniciar los sistemas de los equipos de computación, ni conectar o manipular los dispositivos de almacenamiento que pudieran ubicarse adyacentes, ya que esto supone una alteración y/o modificación de la información o data que podría constituirse como evidencia posteriormente.

- No deberán apagarse los sistemas que se encuentren ya iniciados, ya que eventualmente pudieran requerir ser analizados a través de procedimientos forenses especiales (volcado de memoria, levantamiento de información en vivo, entre otros) por parte del experto.

Procedimientos Asociados al Proceso de Fijación

- Se deberá identificar y reseñar el lugar donde se halla la o las evidencias, a su vez se fijará fotográficamente con exactitud.

- En los casos que se requiera dejar constancia de detalles u observaciones más puntuales, se deberá utilizar testigo flecha (indicador) y/o testigo métrico (de ser necesario).

Procedimientos Asociados al Proceso de Colección

Para aquellos dispositivos (equipos de computación, dispositivos de almacenamiento, equipos o dispositivos de comunicación, etc…) que se encuentren apagados, se deberá cumplir el siguiente procedimiento:

1. Desconectarlos cuidadosamente, en caso de que estén unidos en red o a otros dispositivos, a fuente de poder o tengan periféricos conectados.

2. Cuando se trate de dispositivos de almacenamiento electrónicos y electro-magnéticos, se deberá ejecutar una función criptográfica HASH sobre el dispositivo en específico.

Lógicamente, la colección debe realizarla un experto que a su vez elegirá el algoritmo criptográfico que considere pertinente e idóneo.

Procedimientos Asociados al Proceso de Embalaje

Los dispositivos serán embalados con bolsas de plástico protectoras (de ser posible de burbujas de aire), anime o cartón, con la finalidad de evitar las vibraciones de los componentes electrónicos y electro-magnéticos internos, ya que dicha puede afectar la funcionalidad de los mismos.

Procedimientos Asociados al Proceso de Traslado

A la hora trasladar este tipo de evidencias, es necesario tratarla con sumo cuidado contra las causales expuestas anteriormente, es decir, golpes, manipulaciones incorrectas, factores ambientales y de campos magnéticos.

Procedimientos Asociados al Proceso de Resguardo

Este tipo de evidencia debe resguardarse en condiciones que garanticen su seguridad e integridad, tomando en consideración lo expuesto en títulos anteriores acerca de la protección contra factores ambientales, campos magnéticos, caídas, golpes, entre otros.

Por razones lógicas, este proceso se extiende hasta el Proceso de Peritación. Es necesario garantizar la integridad de éstas durante todo el proceso, desde antes que el experto realice su análisis y en los casos que aplique, hasta después que se realiza el mismo.

Procedimiento recomendado para la adquisición y resguardo de Evidencia Directamente informática o digital

Normalmente este procedimiento constituye lo que en materia de Cadena de Custodia venezolana denominamos "Proceso de Obtención por derivación", pues de la Evidencia física con carácter digital deriva este tipo de evidencia. Este procedimiento se realiza en la segunda fase de la Cadena de custodia, es decir, en el proceso de Peritación.

Principios durante la colección de evidencias

1. Capturar una imagen del sistema tan precisa como sea posible.
2. Realizar notas detalladas, incluyendo fechas y horas indicando si se utiliza horario local o UTC.
3. Minimizar los cambios en la información que se está recolectando y eliminar los agentes externos que puedan hacerlo.
4. En el caso de enfrentarse a un dilema entre recolección y análisis elegir primero recolección y después análisis.
5. Recoger la información según el orden de volatilidad (de mayor a menor).
6. Tener en cuenta que por cada dispositivo la recogida de información puede realizarse de distinta manera.

Orden de volatilidad

Los expertos utilizan esta terminología para hacer referencia al período de tiempo durante el cual será accesible cierta información. Por tal motivo, se debe recolectar prioritariamente aquella

información que esté disponible durante el menor período de tiempo, es decir, aquella cuya volatilidad sea mayor, por ejemplo, el registros y contenido de la caché.

Acciones que deben evitarse durante el Procedimiento

Tomando en consideración que los resultados obtenidos de la investigación serán utilizados en un Proceso judicial y por lo tanto la información debe preservarse íntegramente, se deben evitar las siguientes practicas:

- No apagar el equipo hasta que se haya recopilado toda la información volátil.

- No confiar en la información proporcionada por los programas del sistema ya que pueden haberse visto comprometidos. Se debe recopilar la información mediante programas desde un medio protegido (se explicará a profundidad más adelante).

- No ejecutar programas que modifiquen la fecha y hora de acceso de todos los ficheros del sistema.

Herramientas necesarias para el Procedimiento

Existen una serie de pautas que deben de ser seguidas a la hora de seleccionar las herramientas con las que se va a llevar a cabo el proceso de recolección:

- Se deben utilizar herramientas ajenas al sistema ya que éstas pueden haberse visto comprometidas.

- Se debe procurar utilizar herramientas que alteren lo menos posible el escenario, evitando, en la medida de lo posible, el uso de herramientas de interfaz gráfico y aquellas cuyo uso de memoria sea grande.
- Los programas que se vayan a utilizar para recolectar las evidencias deben estar ubicados en un dispositivo de sólo lectura (CDROM, USB, etc.).
- Se debe preparar un conjunto de utilidades adecuadas a los sistemas operativos con los que se trabaje.
- El kit de análisis debe incluir, entre otros, los siguientes tipos de herramientas: Programas para listar y examinar procesos. Programas para examinar el estado del sistema. Programas para realizar copias bit a bit.

Procedimiento de colección

El procedimiento de colección debe de ser lo más detallado posible, procurando que no sea ambiguo y reduciendo al mínimo la toma de decisiones. Una de las características fundamentales de este procedimiento consiste en que los métodos utilizados para recolectar evidencias deben de ser transparentes y reproducibles. Además, dichos métodos deben haber sido comprobados por expertos independientes.

Fases

1. Listar qué sistemas están involucrados en el incidente y de cuáles de ellos se deben tomar evidencias.

2. Establecer qué es relevante. Sin embargo, en caso de duda es mejor recopilar mucha información que poca.
3. Fijar el orden de volatilidad para cada sistema.
4. Obtener la información de acuerdo al orden establecido.
5. Comprobar el grado de sincronización del reloj del sistema.
6. Según se vayan realizando los pasos de recolección preguntarse qué más puede ser una evidencia.

Es de suma importancia registrar y documentar cada paso.

Procedimiento de almacenamiento

Debido al carácter delicado de la materia es necesario indicar:

• ¿Dónde?, ¿cuándo? y ¿quién? descubrió y recolectó la evidencia.

• ¿Dónde?, ¿cuándo? y ¿quién? manejó la evidencia.

• ¿Quién ha custodiado la evidencia?, ¿cuánto tiempo? y ¿cómo la ha almacenado?

• En el caso de que la evidencia cambie de custodia indicar cuándo y cómo se realizó el intercambio, incluyendo número de albarán, etc.

Dónde y cómo almacenarlo

Lógicamente, la información debe almacenarse en dispositivos cuya seguridad haya sido plenamente comprobada y que permitan detectar intentos de acceso no autorizados, con el fin de evitar la contaminación de la evidencia.

Estas anotaciones y las del título anterior constituyen, lo que en Venezuela denominamos **"Proceso de Actividad de Transferencia"** y **"Proceso de Resguardo"** respectivamente, ambos constituyen procesos de carácter continuo en materia de cadena de custodia venezolana.

Bases Jurídicas

- ***Constitución de la República Bolivariana de Venezuela (1999)***

> **"Artículo 48**. Se garantiza el secreto e inviolabilidad de las comunicaciones privadas en todas sus formas. No podrán ser interferidas sino por orden de un tribunal competente, con el cumplimiento de las disposiciones legales y preservándose el secreto de lo privado que no guarde relación con el correspondiente proceso.
>
> **Artículo 49.** El debido proceso se aplicará a todas las actuaciones judiciales y administrativas; en consecuencia:
>
> 1. La defensa y la asistencia jurídica son derechos inviolables en todo estado y grado de la investigación y del proceso. Toda persona tiene derecho a ser notificada de los cargos por los cuales se le investiga, de acceder a las pruebas y de disponer del tiempo y de los medios adecuados para ejercer su defensa. Serán nulas las pruebas obtenidas mediante violación del debido proceso. Toda persona declarada culpable tiene derecho a recurrir del fallo, con las excepciones establecidas en esta Constitución y la ley…
>
> **Artículo 285.** Son atribuciones del Ministerio Público:
>
> 3. Ordenar y dirigir la investigación penal de la perpetración de los hechos punibles para hacer constar su comisión con todas las circunstancias que puedan influir en la calificación y responsabilidad de los autores o las autoras y demás participantes, así como el aseguramiento de los objetos activos y pasivos relacionados con la perpetración…**"**

- ***Convenio de la Organización Mundial de la Propiedad Intelectual (1967)***

  "**Articulo N.º 2**

  (VIII) "Propiedad intelectual", los derechos relativos:

  - a las obras literarias, artísticas y científicas.

  - a las interpretaciones de los artistas intérpretes y a las ejecuciones de los artistas ejecutantes, a los fonogramas y a las emisiones de radiodifusión.

  - a las invenciones en todos los campos de la actividad humana.

  - a los descubrimientos científicos.

  - a los dibujos y modelos industriales.

  - a las marcas de fábrica, de comercio y de servicio, así como a los nombres y denominaciones comerciales.

  - a la protección contra la competencia desleal, y todos los demás derechos relativos a la actividad intelectual en los terrenos industrial, científico, literario y artístico."

- ***Código Procesal Penal Venezolano (2021)***

  "Licitud de la Prueba

  Artículo 181. Los elementos de convicción sólo tendrán valor si han sido obtenidos por un medio lícito e incorporados al proceso conforme a las disposiciones de este Código. No podrá utilizarse información obtenida mediante tortura, maltrato, coacción, amenaza, engaño, indebida intromisión en la intimidad del domicilio, en la correspondencia, las comunicaciones, los papeles y los archivos privados, ni la obtenida por otro medio que menoscabe la voluntad o viole los derechos fundamentales de las personas. Asimismo, tampoco podrá apreciarse la información que provenga directa o indirectamente de un medio o procedimiento ilícitos. El Juez o Jueza procurará sanear el acto antes de declarar la nulidad de las actuaciones.

Libertad de Prueba

Artículo 182. Salvo previsión expresa en contrario de la ley, se podrán probar todos los hechos y circunstancias de interés para la correcta solución del caso y por cualquier medio de prueba, incorporado conforme a las disposiciones de este Código y que no esté expresamente prohibido por la ley. Regirán, en especial, las limitaciones de la ley relativas al estado civil de las personas. Un medio de prueba, para ser admitido, debe referirse, directa o indirectamente, al objeto de la investigación y ser útil para el descubrimiento de la verdad. Los tribunales podrán limitar los medios de prueba ofrecidos para demostrar un hecho o una circunstancia, cuando haya quedado suficientemente comprobado con las pruebas ya practicadas. El tribunal puede prescindir de la prueba cuando ésta sea ofrecida para acreditar un hecho notorio.

Presupuesto de la Apreciación

Artículo 183. Para que las pruebas puedan ser apreciadas por el tribunal, su práctica debe efectuarse con estricta observancia de las disposiciones establecidas en este Código.

Cadena de custodia

Artículo 187. Todo funcionario o funcionaria que colecte evidencias físicas debe cumplir con la cadena de custodia, entendiéndose por ésta, la garantía legal que permite el manejo idóneo de las evidencias digitales, físicas o materiales, con el objeto de evitar su modificación, alteración o contaminación desde el momento de su ubicación en el sitio del suceso o lugar del hallazgo, su trayectoria por las distintas dependencias de investigaciones penales, criminalísticas y forenses, la consignación de los resultados a la autoridad competente, hasta la culminación del proceso.

La cadena de custodia comprende el procedimiento empleado en la inspección técnica del sitio del suceso y del cadáver si fuere el caso, debiendo cumplirse progresivamente con los pasos de protección, fijación, colección, embalaje, rotulado, etiquetado, preservación y traslado de las evidencias a las respectivas dependencias de investigaciones penales, criminalísticas y ciencias forenses, u órganos jurisdiccionales.

Los funcionarios o funcionarias que colectan evidencias físicas deben registrarlas en la planilla diseñada para la cadena de custodia, a fin de garantizar la integridad, autenticidad, originalidad y seguridad del elemento probatorio, desde el momento de su colección, trayecto dentro de las distintas dependencias de investigaciones penales, criminalísticas y ciencias forenses, durante su presentación en el debate del juicio oral y público, hasta la culminación del proceso.

La planilla de registro de evidencias físicas deberá contener la indicación, en cada una de sus partes, de los funcionarios o funcionarias, o personas que intervinieron en el resguardo, fijación fotográfica o por otro medio, colección, embalaje, etiquetaje, traslado, preservación, análisis, almacenaje y custodia de evidencias físicas, para evitar

y detectar cualquier modificación, alteración, contaminación o extravío de estos elementos probatorios.

Los procedimientos generales y específicos, fundados en los principios básicos de la cadena de custodia de las evidencias físicas, estarán regulados por un manual de procedimiento único, de uso obligatorio para todas las instituciones policiales del territorio nacional, que practiquen entre sus labores, el resguardo, fijación fotográfica o por otro medio, colección, embalaje, etiquetaje, traslado, preservación, análisis, almacenaje y custodia de evidencias físicas, con la finalidad de mantener un criterio unificado de patrones criminalísticos. El referido Manual de Procedimientos en Materia de Cadena de Custodia de Evidencias Físicas, es competencia del Ministerio del Poder Popular para Relaciones Interiores y Justicia en coordinación con el Ministerio Público.

Apreciación de las Pruebas

Artículo 22. Las pruebas se apreciarán por el tribunal según la sana crítica observando las reglas de la lógica, los conocimientos científicos y las máximas de experiencia.**"**

- ***Ley especial contra los Delitos Informáticos (2001)***

"Acceso indebido

Artículo 6. Toda persona que sin la debida autorización o excediendo la que hubiere obtenido, acceda, intercepte, interfiera o use un sistema que utilice tecnologías de información, será penado con prisión de uno a cinco años y multa de diez a cincuenta unidades tributarias.

Sabotaje o daño a sistemas

Artículo 7. Todo aquel que con intención destruya, dañe, modifique o realice cualquier acto que altere el funcionamiento o inutilice un sistema que utilice tecnologías de información o cualesquiera de los componentes que lo conforman, será penado con prisión de cuatro a ocho años y multa de cuatrocientas a ochocientas unidades tributarias. Incurrirá en la misma pena quien destruya, dañe, modifique o inutilice la data o la información contenida en cualquier sistema que utilice tecnologías de información o en cualesquiera de sus componentes.

La pena será de cinco a diez años de prisión y multa de quinientas a mil unidades tributarias, si los efectos indicados en el presente artículo se realizaren mediante la creación, introducción o transmisión intencional, por cualquier medio, de un virus o programa análogo.

Favorecimiento culposo del sabotaje o daño

Artículo 8. Si el delito previsto en el artículo anterior se cometiere por imprudencia, negligencia, impericia o inobservancia de las normas establecidas, se aplicará la pena correspondiente según el caso, con una reducción entre la mitad y dos tercios.

Acceso indebido o sabotaje a sistemas protegidos

Artículo 9. Las penas previstas en los artículos anteriores se aumentarán entre una tercera parte y la mitad, cuando los hechos allí previstos o sus efectos recaigan sobre cualesquiera de los componentes de un sistema que utilice tecnologías de información protegido por medidas de seguridad, que esté destinado a funciones públicas o que contenga información personal o patrimonial de personas naturales o jurídicas.

Posesión de equipos o prestación de servicios de sabotaje

Artículo 10. Quien importe, fabrique, distribuya, venda o utilice equipos, dispositivos o programas, con el propósito de destinarlos a vulnerar o eliminar la seguridad de cualquier sistema que utilice tecnologías de información; o el que ofrezca o preste servicios destinados a cumplir los mismos fines, será penado con prisión de tres a seis años y multa de trescientas a seiscientas unidades tributarias.

Espionaje informático

Artículo 11. Toda persona que indebidamente obtenga, revele o difunda la data o información contenidas en un sistema que utilice tecnologías de información o en cualesquiera de sus componentes, será penada con prisión de tres a seis años y multa de trescientas a seiscientas unidades tributarias. La pena se aumentará de un tercio a la mitad, si el delito previsto en el presente artículo se cometiere con el fin de obtener algún tipo de beneficio para sí o para otro.

El aumento será de la mitad a dos tercios, si se pusiere en peligro la seguridad del Estado, la confiabilidad de la operación de las instituciones afectadas o resultare algún daño para las personas naturales o jurídicas, como consecuencia de la revelación de las informaciones de carácter reservado.

Falsificación de documentos

Artículo 12. Quien, a través de cualquier medio, cree, modifique o elimine un documento que se encuentre incorporado a un sistema que utilice tecnologías de información; o cree, modifique o elimine datos del mismo; o incorpore a dicho sistema un documento inexistente, será penado con prisión de tres a seis años y multa de trescientas a seiscientas unidades tributarias. Cuando el agente hubiere actuado con el fin de procurar para sí o para otro algún tipo de beneficio, la pena se aumentará entre

un tercio y la mitad. El aumento será de la mitad a dos tercios si del hecho resultare un perjuicio para otro.

Fraude

Artículo 14. Todo aquel que, a través del uso indebido de tecnologías de información, valiéndose de cualquier manipulación en sistemas o cualquiera de sus componentes, o en la data o información en ellos contenida, consiga insertar instrucciones falsas o fraudulentas, que produzcan un resultado que permita obtener un provecho injusto en perjuicio ajeno, será penado con prisión de tres a siete años y multa de trescientas a setecientas unidades tributarias.

Obtención indebida de bienes o servicios

Artículo 15. Quien, sin autorización para portarlos, utilice una tarjeta inteligente ajena o instrumento destinado a los mismos fines, o el que utilice indebidamente tecnologías de información para requerir la obtención de cualquier efecto, bien o servicio; o para proveer su pago sin erogar o asumir el compromiso de pago de la contraprestación debida, será castigado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias.

Manejo fraudulento de tarjetas inteligentes o instrumentos análogos

Artículo 16. Toda persona que por cualquier medio cree, capture, grabe, copie, altere, duplique o elimine la data o información contenidas en una tarjeta inteligente o en cualquier instrumento destinado a los mismos fines; o la persona que, mediante cualquier uso indebido de tecnologías de información, cree, capture, duplique o altere la data o información en un sistema, con el objeto de incorporar usuarios, cuentas, registros o consumos inexistentes o modifique la cuantía de éstos, será penada con prisión de cinco a diez años y multa de quinientas a mil unidades tributarias.

En la misma pena incurrirá quien, sin haber tomado parte en los hechos anteriores, adquiera, comercialice, posea, distribuya, venda o realice cualquier tipo de intermediación de tarjetas inteligentes o instrumentos destinados al mismo fin, o de la data o información contenidas en ellos o en un sistema.

Apropiación de tarjetas inteligentes o instrumentos análogos

Artículo 17. Quien se apropie de una tarjeta inteligente o instrumento destinado a los mismos fines, que se haya perdido, extraviado o que haya sido entregado por equivocación, con el fin de retenerlo, usarlo, venderlo o transferirlo a una persona distinta del usuario autorizado o entidad emisora, será penado con prisión de uno a cinco años y multa de diez a cincuenta unidades tributarias. La misma pena se impondrá a quien adquiera o reciba la tarjeta o instrumento a que se refiere el presente artículo.

Provisión indebida de bienes o servicios

Artículo 18. Todo aquel que, a sabiendas de que una tarjeta inteligente o instrumento destinado a los mismos fines, se encuentra vencido, revocado; se haya indebidamente obtenido, retenido, falsificado, alterado; provea a quien los presente de dinero, efectos, bienes o servicios, o cualquier otra cosa de valor económico será penado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias.

Posesión de equipo para falsificaciones

Artículo 19. Todo aquel que sin estar debidamente autorizado para emitir, fabricar o distribuir tarjetas inteligentes o instrumentos análogos, reciba, adquiera, posea, transfiera, comercialice, distribuya, venda, controle o custodie cualquier equipo de fabricación de tarjetas inteligentes o de instrumentos destinados a los mismos fines, o cualquier equipo o componente que capture, grabe, copie o transmita la data o información de dichas tarjetas o instrumentos, será penado con prisión de tres a seis años y multa de trescientas a seiscientas unidades tributarias.

Violación de la privacidad de la data o información de carácter personal

Artículo 20. Toda persona que intencionalmente se apodere, utilice, modifique o elimine por cualquier medio, sin el consentimiento de su dueño, la data o información personales de otro o sobre las cuales tenga interés legítimo, que estén incorporadas en un computador o sistema que utilice tecnologías de información, será penada con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias. La pena se incrementará de un tercio a la mitad si como consecuencia de los hechos anteriores resultare un perjuicio para el titular de la data o información o para un tercero.

Violación de la privacidad de las comunicaciones

Artículo 21. Toda persona que mediante el uso de tecnologías de información acceda, capture, intercepte, interfiera, reproduzca, modifique, desvíe o elimine cualquier mensaje de datos o señal de transmisión o comunicación ajena, será sancionada con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias.

Revelación indebida de data o información de carácter personal

Artículo 22. Quien revele, difunda o ceda, en todo o en parte, los hechos descubiertos, las imágenes, el audio o, en general, la data o información obtenidos 6 por alguno de los medios indicados en los artículos 20 y 21, será sancionado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias. Si la revelación, difusión

o cesión se hubieren realizado con un fin de lucro, o si resultare algún perjuicio para otro, la pena se aumentará de un tercio a la mitad.

Difusión o exhibición de material pornográfico

Artículo 23. Todo aquel que, por cualquier medio que involucre el uso de tecnologías de información, exhiba, difunda, transmita o venda material pornográfico o reservado a personas adultas, sin realizar previamente las debidas advertencias para que el usuario restrinja el acceso a niños, niñas y adolescentes, será sancionado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias.

Exhibición pornográfica de niños o adolescentes

Artículo 24. Toda persona que por cualquier medio que involucre el uso de tecnologías de información, utilice a la persona o imagen de un niño, niña o adolescente con fines exhibicionistas o pornográficos, será penada con prisión de cuatro a ocho años y multa de cuatrocientas a ochocientas unidades tributarias.

Apropiación de propiedad intelectual

Artículo 25. Quien sin autorización de su propietario y con el fin de obtener algún provecho económico, reproduzca, modifique, copie, distribuya o divulgue un software u otra obra del intelecto que haya obtenido mediante el acceso a cualquier sistema que utilice tecnologías de información, será sancionado con prisión de uno a cinco años y multa de cien a quinientas unidades tributarias.

Oferta engañosa

Artículo 26. Toda persona que ofrezca, comercialice o provea de bienes o servicios, mediante el uso de tecnologías de información, y haga alegaciones falsas o atribuya características inciertas a cualquier elemento de dicha oferta, de modo que pueda resultar algún perjuicio para los consumidores, será sancionada con prisión de uno a cinco años y multa de cien a quinientas unidades tributarias, sin perjuicio de la comisión de un delito más grave."

- ***Ley orgánica contra la Delincuencia Organizada y Financiamiento al terrorismo***

"Artículo N. º4

A los efectos de esta Ley, se entiende por:

1. Acto terrorista: es aquel acto intencionado que por su naturaleza o su contexto, pueda perjudicar gravemente a un país o a una organización internacional tipificado como delito según el ordenamiento jurídico venezolano, cometido con el fin de

intimidar gravemente a una población; obligar indebidamente a los gobiernos o a una organización internacional a realizar un acto o a abstenerse de hacerlo; o desestabilizar gravemente o destruir las estructuras políticas fundamentales, constitucionales, económicas o sociales de un país o de una organización internacional.

Serán considerados actos terroristas los que se realicen o ejecuten a través de los

siguientes medios:

a. atentados contra la vida de una persona que puedan causar la muerte;

b. atentados contra la integridad física de una persona;

c. secuestro o toma de rehenes;

d. causar destrucciones masivas a un gobierno o a instalaciones públicas, sistemas de transporte, infraestructuras, incluidos los sistemas de información, plataformas fijas o flotantes emplazadas en la zona económica exclusiva o en la plataforma continental, lugares públicos o propiedades privadas que puedan poner en peligro vidas humanas o producir un gran perjuicio económico;

e. apoderamiento de aeronaves y de buques o de otros medios de transporte colectivo, o de mercancías;

f. fabricación, tenencia, adquisición, transporte, suministro, desarrollo o utilización de armas de fuego, explosivos, armas nucleares, biológicas y químicas;

g. liberación de sustancias peligrosas, o provocación de incendios, inundaciones o explosiones cuyo efecto sea poner en peligro vidas humanas;

h. perturbación o interrupción del suministro de agua, electricidad u otro recurso natural fundamental cuyo efecto sea poner en peligro vidas humanas.

Pornografía

Artículo 46. Quien como parte integrante de un grupo de delincuencia organizada explote la industria o el comercio de la pornografía para reproducir lo obsceno o impúdico a fin de divulgarlo al público en general, será penado o penada con prisión de diez a quince años. Si la pornografía fue realizada con niños, niñas o adolescentes o para ellos, será penado o penada con prisión de veinticinco a treinta años de prisión.

Difusión de material pornográfico

Artículo 47. Quien, como parte integrante de un grupo de delincuencia organizada por cualquier medio directo o indirecto, venda, difunda o exhiba material pornográfico a niños, niñas o adolescentes, será penado o penada con prisión de veinticinco a treinta años.

Utilización de niños, niñas o adolescentes en la pornografía

Artículo 48. Quien como parte integrante de un grupo de delincuencia organizada utilice a niños, niñas o adolescentes o su imagen, con fines o en 24 espectáculos exhibicionistas o pornográficos, tanto públicos como privados, o para elaborar cualquier clase de material pornográfico, cualquiera que sea su soporte, o financie cualquiera de estas actividades, será penado o penada con prisión de veinticinco a treinta años.

Elaboración de material pornográfico infantil

Artículo 49. Quien como parte integrante de un grupo de delincuencia organizada produzca, venda, distribuya, exhiba o facilite la producción, venta, difusión o exhibición por cualquier medio de material pornográfico, en cuya elaboración hayan sido utilizados niños, niñas o adolescentes, aunque el material tenga su origen en el extranjero o fuese desconocido, será penado o penada con prisión de veinte a veinticinco años.**"**

El Convenio de Budapest sobre la Ciberdelincuencia

Es considera la norma internacional más completa hasta la fecha, proporciona un marco integral y coherente en contra del ciberdelito y la evidencia electrónica. Sirve como una guía para cualquier país que desea desarrollar una legislación nacional integral sobre ciberdelitos.

El Convenio de Budapest prevé:

- La criminalización de la conducta, que va desde el acceso ilícito, ataques a la integridad del sistema y de los datos hasta el fraude informático y los delitos relacionados con la pornografía infantil.

- Una serie herramientas de derecho procesal para hacer más efectiva la investigación relacionada con ciberdelitos y la obtención de evidencias electrónicas.

- Una cooperación internacional más ágil y eficiente para la persecución de los delitos cibernéticos. El tratado está abierto para la adhesión de cualquier país.

Cabe destacar que este instrumento normativo se utilizó como fuente doctrinal, pues la República Bolivariana de Venezuela no forma parte del precitado convenio.

Términos básicos

1. ***Evidencia Digital:*** Es todo aquel dato informático avanzado o dispositivo con carácter digital o electrónico que pueda ser de utilidad para el esclarecimiento de hechos punibles.

2. ***Evidencia física con carácter digital o electrónico:*** hace referencia a dispositivos electrónicos o hardware que por su naturaleza contienen material informático como, por ejemplo: discos duros, pendrives, teléfonos inteligentes, etc.

3. ***Evidencia directamente digital:*** corresponde a la información almacenada en la red, hardware o dispositivos electrónicos. Algunos ejemplos de evidencias digitales son: Correos Electrónicos, Documentos Digitalizados, Firmas Digitales, Fichero en disco, proceso en ejecución, Log, Archivos temporales, Entradas de registro, etc.

4. ***Hardware:*** Conjunto de elementos físicos o materiales que constituyen una computadora o un sistema informático.

5. ***Software:*** Conjunto de programas y rutinas que permiten a la computadora realizar determinadas tareas.

6. ***Malware:*** Es un término compuesto, que conjuga las palabras "Malicious software" (software malicioso) y hace referencia a cualquier tipo de software diseñado para infiltrarse en dispositivos sin el conocimiento ni el consentimiento de su propietario.

7. ***Almacenamiento Interno:*** Se refiere a los dispositivos que permiten grabar la información que generalmente se encuentra en la RAM, y que tanto el usuario como el sistema operativo, disponen de ellos para su trabajo y operación diarios. Este tipo de almacenamiento como no volátil, es decir, que el usuario puede guardar sus programas e información con la seguridad de que no se borrarán aun cuando la computadora no esté encendida.

8. ***Memoria RAM:*** La RAM es la memoria principal (Random Access Memory o Memoria de Acceso Aleatorio) y corresponde al espacio de trabajo del procesador central de una computadora. El término "espacio de trabajo" también es utilizado debido a que dicho espacio está activo mientras la computadora esté encendida y en ejecución. En efecto, la memoria principal es volátil, es decir, la información y las instrucciones (software) permanecerán temporalmente mientras la computadora esté en operación de tal forma que, cuando se apague, tanto la información como los programas desaparecerán de la RAM.

9. ***Caché:*** En informática, una memoria caché es una capa de almacenamiento de datos de alta velocidad que almacena un subconjunto de datos, normalmente transitorios, de modo que las solicitudes futuras de dichos datos se atienden con mayor rapidez, los datos en una memoria caché suelen almacenarse en hardware de acceso rápido, como la memoria de acceso aleatorio

(RAM) y también puede utilizarse junto con un componente de software. El objetivo principal de la caché es aumentar el rendimiento de recuperación de datos para evitar tener que acceder a la capa subyacente de almacenamiento, que es más lenta.

Al intercambiar capacidad por velocidad, una memoria caché normalmente almacena un subconjunto de datos de forma transitoria, a diferencia de las bases de datos cuyos elementos suelen ser completos y duraderos.

10. ***Fichero (archivo):*** Es un conjunto ordenado de datos que tienen entre si una relación lógica, que están almacenados en un soporte de información compatible con el dispositivo en el que residen. Los ficheros almacenan información referente a un mismo tema de manera organizada con la finalidad de manipular los datos que contienen, individualmente.

11. ***Fichero Manual:*** Es todo conjunto de datos de carácter personal organizado de forma no automatizada y estructurado conforme a criterios específicos relativos a personas físicas.

12. ***Fichero Automatizado:*** Son aquellos ficheros que guardan los datos de carácter personal en soportes informatizados**,** a los que se accede, a su vez, mediante programas o sistemas informáticos. Esta facilidad y potencia de acceso que permite la tecnología informática ha dado lugar a la actual legislación de protección de datos personales, que no era necesaria cuando el acceso a esos datos se efectuaba manualmente. Una gran parte de la actual legislación y normativa al respecto está dedicada a este tipo de ficheros.

13. ***Ficheros Mixtos:*** Este tipo de ficheros va a mezclar un acceso informatizado e incluso, una grabación informatizada de una parte de los datos, con un almacenamiento de datos en soportes no informáticos.

14. ***Protocolo de control de transmisión/Protocolo de Internet (TCP/IP):*** Es un conjunto de reglas estandarizadas que permiten a los equipos comunicarse en una red como Internet. El TCP e IP son dos protocolos distintos para redes informáticas. **IP** es la parte que obtiene la dirección a la que se envían los datos. **TCP** se encarga de la entrega de los datos una vez hallada dicha dirección IP.

15. ***Dirección IP:*** Significa (Dirección del Protocolo de Internet), consiste en un conjunto de reglas que regulan la comunicación a través de Internet, las direcciones IP identifican una red o el dispositivo específico que se encuentre activo en la misma.

16. ***Dirección IP Pública:*** Consiste en aquella dirección IP que nos asigna nuestro proveedor de servicios de Internet (ISP).

17. ***Dirección IP Privada: Sirve para*** identificar dispositivos dentro de una red doméstica o una oficina. La dirección IP local o privada es asignada automáticamente por el Router, que es el hardware que conecta una red local a Internet.

18. ***Hash:*** Una función criptográfica Hash, es un algoritmo matemático que transforma cualquier bloque de datos en una nueva serie de caracteres con una longitud fija. Independientemente de la longitud de los datos de entrada, el valor hash de salida tendrá siempre la misma longitud.

19. ***DNS:*** El sistema de nombres de dominio (DNS) por analogía podría considerarse el directorio telefónico de Internet. Los navegadores web interactúan mediante direcciones de Protocolo de Internet (IP), las personas navegan a valiéndose de nombres de dominio como "www.espn.com" u otros ejemplos. El DNS traduce los nombres de dominio a direcciones IP, por ende, los servidores DNS suprimen la necesidad de que los humanos memoricen direcciones IP, las cuales suelen ser complejas al combinar caracteres alfanuméricos.

Capítulo III: Marco Metodológico

La presente Investigación es de tipo documental, cualitativo y cuenta con un diseño no experimental. Nuestro proceso de investigación lo hemos realizado con la búsqueda y análisis de información extraída de fuentes como: libros, Internet, material impreso, entre otras cosas, las cuales han sido registradas por otros investigadores.

El método documental o bibliográfico consiste en la captación de datos, con el fin de construir a través del análisis crítico procesos coherentes de aprehensión y compresión del fenómeno objeto de estudio. A su vez estamos desarrollando una investigación de tipo Cualitativo por eso nos centramos en comprender un fenómeno desde una perspectiva natural, tomando en consideración el significado que le otorgan las personas implicadas. Como se ha indicado con anterioridad se trata de una investigación realizada en contacto directo con los documentos físicos y digitales en recinto cerrado, por ende, es totalmente diferente a una investigación de campo. Según **Fidias Arias (2006)** la Investigación Documental consiste en:

> "la investigación documental es un **proceso basado en la búsqueda, recuperación, análisis, críticas e interpretación de datos secundarios**, es decir los obtenidos y registrados por otros investigadores en fuentes documentales: impresas, audiovisuales o electrónicas".

A su vez **Consuelo Hoyos Botero** opina respecto de la investigación documental lo siguiente:

> "Es un trabajo constitutivo donde la interpretación, la crítica y la argumentación racional, juegan un papel preponderante porque permiten llevar a cabo inferencias y relaciones. Se trata de ir de la parte (unidad de análisis) al todo (fenómeno estudiado a través de la representación teórica), para explicitar un argumento de sentido que explique y totalice una cierta visión "paradigmática, semántica y pragmática" en orden a dilucidar una particular manera de apreciar el fenómeno, una construcción global de significados y una trascendencia en lo real de estos elementos con repercusiones prácticas en el entorno social"

Fases de la Investigación

1. **Fase I: Identificar la metodología aplicada actualmente por los organismos policiales y de investigación penal para garantizar la integridad de las evidencias de carácter digital y su idoneidad.**

Para desarrollar este objetivo, se realizó un estudio documental partiendo del análisis del contenido del Manual Único de cadena de custodia vigente, estudios, recomendaciones y guías metodológicas desarrolladas internacionalmente, a su vez se realizó una amplia lectura de material periodístico, con contenido relativo a delitos informáticos y su judicialización, con esto se pretende identificar la metodología aplicada y luego concatenarla con los estándares internacionales en la materia.

2. **Fase II: Precisar si existe en el Manual único de Cadena de custodia vigente, una serie de procedimientos estandarizados que garanticen el manejo adecuado de la evidencia digital.**

Se realizará una revisión íntegra y profunda de lo expuesto en el vigente Manual Único de Cadena de custodia de evidencias físicas (2017), sin embargo, debido a la importancia del tópico desarrollado en el presente trabajo investigativo, no solo se analizará el contenido del texto precitado, sino que también se analizará el contenido del Manual Único de Procedimientos en materia de Cadena de custodia de evidencias físicas (2012), escrito que fungió como antecesor al manual vigente y que debido a la riqueza de áreas de interés criminalístico que desarrolla sigue teniendo peso fáctico en el campo de la investigación Penal y criminalístico.

3. Fase III: Concientizar acerca del valor Probatorio de las evidencias digitales en el Proceso Penal Venezolano para el esclarecimiento y Judicialización de hechos punibles.

Mediante el desarrollo en sí mismo del presente trabajo se completó este objetivo, pues con el se pretende orientar a la comunidad científica, técnica y académica, con la finalidad de propiciar una tendencia ascendente en cuanto al desarrollo de información científica que exponga cual es la manera idónea de tratar esta materia, que a su vez permitirá concientizar sobre la importancia de este descuidado tópico, ubicado específicamente dentro de la esfera del Derecho Penal venezolano.

Capítulo IV: Resultados, Conclusiones y Recomendaciones

Resultados

1. **Fase I: Identificar la metodología aplicada actualmente por los organismos policiales y de investigación penal para garantizar la integridad de las evidencias de carácter digital y su idoneidad.**

Realizado el análisis documentológico correspondiente, se logró identificar la metodología que aplican los organismos policiales y de investigación penal para garantizar la integridad de las evidencias de carácter digital y su idoneidad. Si bien el Manual Único de Cadena de Custodia vigente, no aporta ningún tipo de contenido metodológico para la obtención técnica y el resguardo de las evidencias con carácter digital o directamente digital, los funcionarios encontraron respuesta a este vacío metodológico, valiéndose del contenido expuesto en el Manual Único de Procedimientos en materia de Cadena de custodia de evidencias físicas del año 2012, el cual desarrolla un procedimiento básico para el manejo de evidencia digital o informática, dicho procedimiento desarrolla respectivamente los Procesos de: Protección, Fijación, Colección, Embalaje, Rotulado, Traslado y Preservación; correspondiente al tipo de evidencia precitada. A su vez indica una serie de experticias realizables en el Área de la informática Forense, las cuales son enunciadas en un sentido No taxativo.

2. **Fase II: Precisar si existe en el Manual único de Cadena de custodia vigente, una serie de procedimientos estandarizados que garanticen el manejo adecuado de la evidencia digital.**

Luego de realizar una revisión íntegra y profunda al contenido del Manual Único de Cadena de custodia de evidencias físicas (2017), el cual lógicamente se encuentra vigente. Se determinó que el mismo no expresa ningún tipo de procedimientos o contenido dirigido a garantizar la preservación y el manejo adecuado de la evidencia digital o informática.

Por contraposición, el Manual Único de Procedimientos en materia de Cadena de custodia de evidencias físicas (2012) si desarrolla una serie un breve procedimiento básico estandarizado dirigido al manejo adecuado de evidencia física con carácter digital o informático, a su vez enuncia una serie de experticias realizables en el área de la informática forense y su fin.

3. Fase III: Concientizar acerca del valor Probatorio de las evidencias digitales en el Proceso Penal Venezolano para el esclarecimiento y Judicialización de hechos punibles.

Culminado el desarrollo del presente trabajo investigativo, se logró abstraer una buena noción teórica y jurídica del status actual de Régimen probatorio venezolano con respecto al manejo de evidencias digitales y las experticias cibernéticas en la materia Penal, lógicamente con la intención de otorgar al lector una experiencia agradable, que facilite su entendimiento y le permita discernir en cuanto a los tópicos planteado.

Igualmente, el presente trabajo investigativo sirve como instrumento para concientizar acerca de la importancia que poseen las evidencias digitales, pues estas constituyen los elementos de convicción más significativos cuando se está en presencia de un Hecho punible de tipo informático, por lo tanto, depende de su correcta valoración la absolución o la culpabilidad de los imputados y consecuentemente la correcta impartición de justicia.

Conclusiones

Finalizado el desarrollo de los objetivos planteados, se proyectaron una serie de conclusiones. Primeramente, en el año 2012 se publicó el Manual Único de Procedimientos en materia de Cadena de custodia de evidencias físicas, un texto lejano a ser perfecto pero que es realmente rico en cuanto a su contenido, pues el mismo desarrolla de forma básica, múltiples áreas específicas relativas al manejo de Evidencia, por ejemplo, el área Toxicológica o el área Documentológica; Sin embargo, lo más resaltante es que el texto precitado, desarrolló un marco metodológico básico para la Evidencia informática o digital, por consiguiente él mismo constituyó un avance en cuanto a la preservación de la evidencia que posteriormente pasaría a constituir material probatorio en los Procesos Judiciales, dando mayor eficacia e idoneidad al Régimen Probatorio venezolano.

Posteriormente, en el año 2017 se publicó el vigente, Manual Único de Cadena de custodia de evidencias física, contrario a lo que podría presumirse, este texto significó un retroceso pues en el mismo se abandonó por completo el contenido metodológico relativo al trato y preservación de la evidencia digital o informática. Esta situación causó un vacío metodológico que se mantiene vigente, para mitigar este vacío la gran mayoría de los Funcionarios Policiales e Investigadores Penales se refugiaron en el procedimiento establecido en el Manual publicado en el año 2012.

Sin embargo, esto causa que el Régimen probatorio venezolano con respecto al manejo de pruebas digitales o informáticas y las experticias cibernéticas, actualmente se encuentre en una situación irregular, que atenta contra el objetivo principal de la publicación de un Manual único y de uso obligatorio en materia de cadena de custodia, que es precisamente regular los procesos, procedimientos, métodos y técnicas, de la cadena de custodia de evidencias relacionadas con un

hecho presuntamente delictivo, con la finalidad de garantizar su integridad desde el momento de su obtención hasta su disposición final.

En este mismo orden de ideas, de forma accesoria esta situación lacera otro de los fines esenciales de un Manual único de cadena de custodia el cual consiste en unificar los criterios de actuación, pues los Funcionarios Policiales, Investigadores Penales y cualquier persona que por razones de sus competencias deba tratar con evidencia, en este caso digital o informática, que conocen la materia aplican de forma supletoria el procedimiento establecido en el Manual del año 2012, quien la conoce de forma parcial inventa un procedimiento vago y quien la desconoce, simple y llanamente no sabe cómo tratar las evidencias al punto de poder atentar contra su integridad de forma culposa.

El Estado representado en este caso por el Ministerio del Poder Popular para Relaciones Interiores, Justicia y Paz en coordinación con el Ministerio Público, debe solventar dicha situación irregular mediante la publicación de un nuevo Manual Único de Cadena de Custodia o un Protocolo anexo al Manual vigente, que dote a la materia informática o digital de un marco metodológico actualizado e idóneo, que permita garantizar la integridad de la evidencia, que posteriormente pasará a constituir material probatorio en los Procesos Judiciales y así, dar mayor efectividad al ejercicio de la garantía fundamental que constituye el derecho a la Justicia.

Recomendaciones

- El Poder Legislativo debe actualizar el contenido normativo que tipifica y sanciona los hechos ilícitos relacionados con el uso de dispositivos y material informático. La norma vigente data del año 2001, los avances tecnológicos desarrollados en fecha posterior a la promulgación de dicha normativa constituyen un hecho innegable.

- El Poder Judicial debe promover la formación académica y la capacitación del personal que conforma nuestro Sistema Judicial, en este caso, las personas que ejercen funciones en el ámbito penal, esto no es taxativo pues el uso fraudulento o delictivo de la tecnología puede presentarse en cualquier controversia jurídica sin importar la materia. Pero de nada vale poseer una normativa actualizada si los Operadores de Justicia no poseen el conocimiento suficiente para su correcta aplicación y defensa.

- El Ministerio del Poder Popular para Relaciones Interiores, Justicia y Paz en coordinación con el Ministerio Público, a ambos designados por la ley como responsables para el desarrollo del Marco metodológico de la trata de evidencia, deben crear un nuevo Manual Único de Cadena de Custodia o un Protocolo anexo al Manual vigente, que cubra íntegramente las falencias en materia de Evidencia informática y digital que presenta el Manual Vigente.

- Los Organismos Policiales y de Investigación Penal y Criminalística, deben crear programas de capacitación en materia de Delitos informáticos, manejo de evidencia informática y digital, y experticias informáticas. Pues si bien el Poder Judicial es quien materializa el mandato de la

ley a partir de las sentencias, los organismos precitados son los encargados de llevar a cabo las averiguaciones mediante las cuales se esclarecen los hechos punibles, que posteriormente el Poder Judicial sancionará. Por esta razón el Personal que los integra debe estar capacitado para la persecución e investigación de cualquier tipo de Hecho punible, A su vez es recomendable la difusión masiva de información dirigida a la ciudadanía con el fin de prevenir Delitos informáticos.

- De igual manera, el Estado cualquiera de sus expresiones, debería proceder a la difusión masiva de información acerca de las posibles entidades de atención que pueden asistir a la ciudadanía a la hora suscitarse algún hecho punible en materia de Delincuencia informática.

- Los Profesionales del Derecho deben educarse en la materia, con el fin de garantizar una defensa adecuada para sus representados, a partir de la promoción de pruebas legales y pertinentes o simplemente solicitando la inadmisión de pruebas digitales o informáticas fraudulentas.

- Es recomendable que la ciudadanía lea y se informe con el fin de prevenir ser víctima de algún delito informático o uso delictivo de la tecnología.

Referencias Bibliográficas

- **Best Practices for seizing Electronic Evidence (2015). Version 4.2. United States Secret Service, U.S. Departament of Homeland Security. Recuperado de file:///C:/Users/HP/Documents/Victor%20Universidad/MANUALES/BestPracticesforSeizingElectronicEvidence.pdf**

- **Constitución de la República Bolivariana de Venezuela (1999). Recuperada de https://www.oas.org/dil/esp/constitucion_venezuela.pdf**

- **Convenio de la Organización Mundial de la Propiedad Intelectual (1967) (Estocolmo). Recuperado de https://wipolex.wipo.int/es/text/283997**

- **Convenio N.º 185, del Consejo de Europa, sobre la Ciberdelincuencia (23 de noviembre de 2001). Recuperado de https://www.oas.org/juridico/english/cyb_pry_convenio.pdf**

- **Código Orgánico Procesal Penal (2021). Recuperado de file:///C:/Users/HP/Documents/Victor%20Universidad/ley-organica-de-reforma-del-codigo-organico-procesal-penal-20211004180004.pdf**

- **Delitos Informáticos: Generalidades (2007) (Ecuador). Autor: Santiago Acurio del Pino. Recuperado de file:///C:/Users/HP/Documents/Victor%20Universidad/cyb_ecu_delitos_inform.pdf**

- **El Tratamiento de la evidencia digital, una guía para su adquisición y/o recopilación. Universidad de Cuenca (Ecuador). (junio, 2018). Autor: Paul A. Ochoa. Recuperado de file:///C:/Users/HP/Documents/Victor%20Universidad/MANUALES/Guia%20Universidad%20de%20Cuenca.pdf**

- **Guía de Toma de evidencias en entornos Windows. Instituto Nacional de Ciberseguridad (INCIBE) (España). (noviembre, 2014).**

- **Guía esencial del phishing: cómo funciona y cómo defenderse (2020). Avast Academy. Autor: Iván Belcic. Recuperado de https://www.avast.com/es-es/c-phishing**

- **Introducción a la Informática Forense (2006). Autor: Jeimy. J. Cano. Recuperado de file:///C:/Users/HP/Documents/Victor%20Universidad/MANUALES/Material%20Jeimy%20Cano.pdf**

- **Manual de Manejo de Evidencias Digitales y Entornos Informáticos (2009). Versión 2.0. Autor: Dr. Santiago Acurio Del Pino. Revista de Derecho Informático.**

Recuperado de file:///C:/Users/HP/Documents/Victor%20Universidad/MANUALES/cyb_pan_manual.pdf

- **Ley especial contra los Delitos Informáticos (30 de octubre de 2001). Recuperada de file:///C:/Users/HP/Documents/Victor%20Universidad/Ley%20Especial%20de%20Delitos%20Informaticos.pdf**

- **¿Qué es el phishing? (2021). Oficia de Seguridad de Internauta (OSI) del Instituto Nacional de Ciberseguridad (INCIBE) (España). Recuperado de https://www.osi.es/es/actualidad/blog/2021/11/17/que-es-el-phishing**

- **¿Qué es un Sniffer y cómo puede protegerse? (2022). Avast Academy. Autor: Iván Belcic. Recuperado de https://www.avast.com/es-es/c-sniffer**

- **¿Qué es un TCP/IP y cómo funciona? (2021). Avast Academy. Autor: Sharon Fisher. Recuperado de https://www.avast.com/es-es/c-what-is-tcp-ip**

- **¿Qué es un deepfake y cómo detectarlo? (2022). Avast Academy. Autor: Carly Burdova. Recuperado de https://www.avast.com/es-es/c-deepfake**