UNIVERSIDAD “LA SALLE”

CARRERA DE DERECHO

“LINEAMIENTOS JURIDICOS PARA EL USO ALGORITMICO EN EL PROCESO DE BUSQUEDA DE LA EVIDENCIA DIGITAL EN DELITOS INFORMATICOS”

POR:

CLEMENCIA ELENA CARRANZA BRAVO

PROFESOR GUÍA:

DR. RUBÉN ALEJANDRO GAMARRA PÉREZ

TESIS PRESENTADA PARA LA OBTENCIÓN DEL GRADO DE LICENCIATURA EN DERECHO

LA PAZ-BOLIVIA 2023

I N D I C E

in memoriam de Roberto Carranza Estivariz

Demostrado pA, la matemática fue, es y será el todo! Mi amor a ti ha descubierto lo infinito.

Paola Carranza Bravo, me hiciste soñar en la magnífica forma de entrelazar a dos ciencias apasionantes; la matemática y el Derecho. Sin ti este trabajo no hubiera sido posible. Gracias!

Agradecimiento:

Mi agradecimiento eterno a mi tutor Doctor Rubén Gamarra Pérez, Jefe de la Carrera de Derecho de la Universidad “La Salle”; por haber sido tan generoso con su valioso tiempo, haberme guiado y brindado sus amplios conocimientos y por haber confiado en mí.

Dedicatoria:

A mi mamita María Elena, hermanos Malu, Pame, Gringuito Roberto(+), Paolita y a mis amados sobrinos Roberto, Luchita, Rene, Luciano, Lucas y Santiago por ser cada uno de ustedes parte de éste sueño.

CAPÍTULO 1

MARCO METODOLOGICO

1.1 Introducción

La transformación de las Tecnologías de la Información y Comunicación (TIC) durante los últimos 30 años ha introducido cambios sustanciales en la forma de vida de las personas de estas generaciones y de esta sociedad; a modo de ejemplo, las nuevas formas de generar negocio a través de las transacciones electrónicas realizadas en el sistema financiero, donde los usuarios ya casi no utilizan el dinero tradicional para realizar una determinada transacción comercial, por el contrario, en las diferentes esferas sociales y empresariales públicas y privadas ya se utiliza – casi de forma exclusiva – el dinero electrónico, bitcoin, billetera digital u otros denominativos que se le dan a los valores monetarios dentro de las TIC.

Sobre esta nueva forma de cómo generar negocio jurídico por medios electrónicos, se han desarrollado nuevas plataformas de convivencia y relacionamiento humano a través del Comercio Electrónico *e-commerce*, Firma Digital, Certificación Electrónica, Correo Electrónico *e-mail*, uso y goce del *Internet* mediante la telefonía celular.

Sobre éste último punto, es importante señalar que según la Autoridad de Tecnología y Telecomunicaciones en la gestión 2017, el crecimiento del uso de *Smartphones* ascendió a 7.939.275 y el acceso a internet en Bolivia el mismo año, alcanzo a 8.817.749 de conexiones fijas y móviles, consecuentemente se puede afirmar que un 79% de la población dentro del territorio nacional cuenta con un *dispositivo* de telefonía celular, con opción al manejo de la cámara fotográfica, filmadora de video o grabadora de voz y otros accesorios que mejoran la calidad del dispositivo en términos comerciales. (ATT, 2018)

Asimismo, estos dispositivos cuentan con el soporte lógico o *Software* y recursos tecnológicos para acceder al *Internet* para la transmisión, emisión y recepción de señales, símbolos, textos, imágenes, video, voz, sonidos, datos o información de cualquier naturaleza o aplicaciones que facilitan los mismos, entre otros. Es por ello, que las diferentes empresas proveedoras del servicio móvil están ofreciendo mejores y mayores servicios de calidad, modernidad, cobertura y precio para capturar mayor cartera de clientes.

Las empresas transnacionales de telecomunicaciones y Tecnología de Información y Comunicación van ofreciendo nuevas alternativas en el mercado digital, sea por parte de *Microsoft* que va desarrollando nuevos modelos y plataformas en el almacenamiento y procesamiento de datos amparados en la licencia de contratos de *Software*, es decir, se atienen a los contratos almacenados en los dispositivos electrónicos lo que, valida el uso, goce y disposición de los recursos tecnológicos contractuales. Por otro lado, está el desarrollo de otras alternativas mediante la explotación del *Software Libre*, es decir, la exposición del *Código Abierto* para que el usuario final pueda acceder, modificar, adecuar y utilizar estos algoritmos de programación sin una regulación contractual.

En consecuencia, partiendo de los principios empresariales para decidir sobre el uso de *Software* con licencia o *Software libre*, las diferentes empresas de servicios comerciales, financieros, empresariales, entre otras como las corporaciones sin y con fines de lucro, están desarrollando y evolucionando exponencialmente nuevos formatos electrónicos para que los usuarios puedan adquirir y acceder a las propuestas de servicios tecnológicos, que se distinguen en: Los servicios comerciales como ser: El comercio electrónico conocido también como *e-commerce*, B2B, B2C, etc.; en los servicios financieros se encuentran las *Transacciones Electrónicas* de toda índole desde el pago de servicios, prestamos, etc.; en los servicios empresariales se tiene una amplia información y así sucesivamente por cada servicio propuesto se tiene a la herramienta o servicio electrónico requerido y distribuido en todas partes del mundo con el único requisito de tener el acceso a *Internet* y, que finalmente concluye en la interrelación empresarial de servicios para generar los bancos de datos, perfiles de usuarios, y otros depositarios de datos e información que lo logra constituirse en el activo más importante dentro de una determinada organización. (González M, 2006)

Las Tecnologías de la Información y Comunicación (TIC), comprenden al conjunto de recursos, herramientas, soportes y canales, redes, medios, que permiten el tratamiento y acceso a la información. El *Internet*, la telefonía móvil y el Sistema de Posicionamiento Global (GPS) pueden considerarse como nuevas TIC. El uso de ordenadores y programas que permiten crear, modificar, almacenar, administrar, proteger y recuperar esa información, como ser: voz, datos, texto, video e imágenes. Se consideran como sus componentes el hardware, el software y los servicios.

Por todo lo mencionado, en sentido positivo, las TIC; se constituyen en una herramienta necesaria e indispensable en el quehacer cotidiano de las personas naturales y de las personas jurídicas. Estas herramientas son desarrolladas y elaboradas mediante la construcción de modelos o algoritmos matemáticos, y como en cualquier modelo, teoría o teorema matemático, también existe el sentido negativo, en especial en las TIC, dónde se están acrecentando exponencialmente las acciones negativas, es decir, en la afectación contra el patrimonio o activo más importante de una organización mediante el uso indebido de las TIC, convergentes con los *Delitos Informáticos* como ser: El acceso indebido, la manipulación informática, la suplantación de identidad, espionaje informático, suplantación indebida de voz, datos, información, texto, imagen o videos en las redes sociales que afectan a un elevado porcentaje de los internautas y otras acciones negativas que se constituyen como acciones antijurídicas, que en algunos casos no está establecidas dentro de nuestra normativa. (Acurio Del Pino, 2006)

Las acciones antijurídicas, donde el sistema periodístico, sistema financiero, sistema comercial y otras instancias administrativas, públicas y privadas, se ven afectadas con la problemática de los riesgos e incidentes legales producidos en el entorno de las TIC está referida al elemento probatorio cuando se ha producido o consumado un acto ilícito en contra del bien jurídico protegido dentro y en torno a las TIC, es decir, ¿Cómo se demuestra la actividad delincuencial y cómo llega a producirse una acción antijurídica en el Estado boliviano? es decir, la *Manipulación Informática* y *Alteración, Acceso y Uso Indebido de datos informáticos* tipificados en los artículos 363 bis y 363 ter del Código Penal boliviano, implica una problemática que se agrava, cuando se suscitan actividades delincuenciales que no están tipificadas como *Delitos Informáticos*; es decir, el espionaje informático, suplantación de identidad, suplantación de voz, sabotaje informático y una amplia actividad delincuencial que no está prevista específicamente en materia penal, aún más cuando no existe una técnica, un método que permita validar los elementos probatorios como es el caso de la *Evidencia Digital*, que no está específicamente reconocida en la ley ni aceptada con todo su alcance en instancias judiciales.

El Código Procesal Penal boliviano no tiene una sección específica en la que se determina la manera correcta de obtener la evidencia digital, ante esta falta de especificidad las

autoridades llamadas por ley a participar de las investigaciones emergentes de un delito en el que se tienen medios tecnológicos propios de la TIC incurren por falta de conocimiento y de guía normativa en errores que terminan por quitarle el valor probatorio potencial que tendría la evidencia digital si se siguiera por lo menos con un protocolo basado en los conocimientos científicos y técnicos contemporáneos.

Cabe hacer notar que en la *Evidencia Digital* se encuentran todos los elementos que demuestran la verdad material de las acciones antijurídicas en contra de las TIC y en éstas se encuentra un código, un algoritmo, un lenguaje de máquina u otro elemento físico o lógico que ha sido desarrollado mediante la construcción de algoritmos matemáticos.

Ante la falta de normas jurídicas o protocolos sobre cómo debe darse el proceso de recolección, análisis e interpretación de la *Evidencia Digital* en un delito informático, la presente investigación busca colaborar con el mejoramiento del sistema jurídico boliviano proponiendo **LINEAMIENTOS JURIDICOS PARA LA INCLUSION DEL USO ALGORITMICO EN EL PROCESO EN LA BUSQUEDA DE LA EVIDENCIA DIGITAL** que permitan garantizar la averiguación de la verdad material cuando se ha producido una acción antijurídica relacionada con el uso de Tecnologías de la Información y Comunicación.

1.2 **Antecedentes**

El avance y crecimiento de los delitos interrelacionados con el exponencial progreso y transformación de las TIC son puntos muy importantes que se van a tomar en cuenta en la presente investigación. Inicialmente es necesario tomar conciencia sobre la frenética progresión de las TIC en sentido positivo y en sentido negativo. La evolución que la sociedad ha ido viviendo en las últimas décadas con los grandes avances tecnológicos que se han convertido en parte del diario vivir de la sociedad en general. La utilización de las computadoras es prácticamente inevitable para realizar actividades diarias, tales como ver las noticias, saber las predicciones del clima, realizar y enviar documentos, hasta el manejo de cajeros automáticos para depositar y sacar sumas de dinero de cuentas bancarias, transacciones monetarias entre distintas entidades financieras mediante la computadora y el

Internet como medio de comunicación y distintas actividades en las que tanto las computadoras como el *Internet* se convierten en herramientas que facilitan la realización de estas actividades. Pero, así como la tecnología es utilizada para el beneficio común de la sociedad, existen personas con altos conocimientos en TIC dedicadas a la realización de actos delictivos en los que se busca el beneficio propio causando daño a las personas naturales y personas jurídicas, y producto de ese alto conocimiento son delitos difíciles de investigar, más difícil aún, encontrar al autor o a los autores, y aún más difícil determinar el cómo se ha producido el evento sin tener el elemento probatorio que demuestre la verdad material de los hechos.

La nomenclatura jurídica, establece la característica típica que posee la acción delincuencial, pero no establece la forma, medio o técnica que debe utilizarse en la *Cadena de Custodia* del proceso de recolección, análisis e interpretación de la *Evidencia Digital*; en consecuencia, se observa que no existe una adecuada disposición legal y vigente al enfoque planteado en la presente investigación.

1.3 **Planteamiento del Problema de Investigación**

Por todo lo expuesto, puede evidenciarse que dentro de la economía jurídica boliviana existe una carencia *en el proceso de búsqueda de la evidencia digital,* problema que es acrecentado por la falta de instituciones jurídicas, técnicas de investigación, metodologías u otra ciencia que sea desarrollada en la formación académica emergente.

En el presente las estadísticas nos indica que entre 2013 y 2020 los delitos informáticos se incrementaron en un 1200 % reflejando un crecimiento desproporcional sobre la comisión de acciones antijurídicas en materia de las TIC, pero el problema es mayor, cuando las instituciones llamadas por ley: Ministerio Público, Investigadores de la Policía, no pueden responder ni accionar ante los ilícitos antes mencionados por la falta de pruebas. (Fondo de Apoyo Periodístico “La Paz y Tarija a través de nuevas miradas”, 2020) y (Fundacion Construir, 2019)

Finalmente, con la presente investigación, se pretende dar el primer paso para reconocer y garantizar la averiguación de la verdad material con validez jurídica y normativa en instancias

judiciales mediante *uso algorítmico en el proceso de búsqueda de la evidencia digital* y para que esta sea reconocida como *prueba* válida e irrefutable en instancias judiciales, en consecuencia, el campo de delimitación del problema será expuesto en los lineamientos jurídicos conforme a los preceptos del *Derecho Informático*.

1.4 **Pregunta de Investigación**

¿Cómo colaborar con la actualización del ordenamiento jurídico procesal boliviano de manera que se mejoren las probabilidades de la averiguación de la verdad material en las acciones antijurídicas en las tecnologías de la Información y Comunicación?

1.5 **Justificación.**

El constante avance de las TIC, permiten introducir nuevas técnicas, formas o medios destinados, en sentido negativo, a la comisión de acciones antijurídicas en ese entorno; por otro lado, muchos de estos tipos de *delitos de cuello blanco* no son investigados ni resueltos en instancias judiciales, por tanto, permiten que los delincuentes no sean sancionados por la comisión de los delitos consumados. (Tellez Aguilera, 2009)

Ante esta debilidad, está presente la inexactitud y generalidad de disposiciones legalmente válidas y aceptadas para el reconocimiento pleno y validez jurídica de la *Evidencia Digital* que permita demostrar la verdad material de los hechos en las acciones antijurídicas en las TIC.

La presente investigación, pretende colaborar a la actualización del ordenamiento jurídico boliviano de manera que se mejoren las probabilidades de la averiguación de la verdad material en las acciones antijurídicas en las Tecnologías de la Información y Comunicación y minimizar la posibilidad de contaminación y desvalorización del elemento probatorio.

1.5.1 **Justificación Económica-Social.**

El avance de la tecnología en cuanto al manejo de las computadoras, Internet y

teléfonos inteligentes, siendo la forma más clara de globalización, son herramientas y dispositivos que están al alcance de toda la sociedad en general, sin hacer discriminación sobre el sexo, la edad, las creencias, raza, idioma u otras características sociales, económicas o estructurales. Pero, así como trae muchos beneficios el uso de éstos, también trae consigo acciones delictivas, malintencionadas. Pues a partir del uso abusivo de las computadoras, el *Internet* y los teléfonos inteligentes, se permite que gente especializada y con gran conocimiento en el área de la informática y telecomunicaciones se aproveche de las personas que son usuarios de estos servicios, engañando de una o de otra manera y obteniendo en muchos casos beneficio propio.

A nivel mundial, hace ya algunos años atrás se ha visto claramente que, a través del *Internet* y el uso de las computadoras se han generado situaciones negativas que atentan contra los derechos y bienes de los usuarios, aspecto por el cual este tipo de acciones se convierten en actos delictivos de última generación y lo peor es que este tipo de situaciones se han vuelto cada vez más comunes.

Ingresando específicamente al ámbito nacional, es necesario entender la necesidad de que Bolivia como Estado tome decisiones sobre el tema para minimizar los riesgos e incidentes legales en el uso indebido de las TIC, de manera que el Estado y las leyes nacionales puedan proteger jurídicamente a su población en general y también castigar mediante penas a las personas delincuentes que dolosamente a través de su conocimiento abusan de éste.

Por esa razón, mediante el análisis que aportará la presente investigación sobre la importancia de proponer **LINEAMIENTOS JURIDICOS PARA EL USO ALGORITMICO EN EL PROCESO DE BUSQUEDA DE LA EVIDENCIA DIGITAL EN DELITOS INFORMATICOS**, se podrá establecer de forma más clara el impacto que tendrá esta contribución al Ordenamiento Jurídico Boliviano, de esta naturaleza que sin duda sería primogénita en su especie dentro del campo del Derecho boliviano, además de demostrar la inseguridad jurídica que atraviesa el país actualmente en éste tema.

1.5.2 **Justificación Jurídica.**

No cabe duda sobre la primacía de la Constitución Política del Estado frente a otras disposiciones de menor rango. La idea subyacente en la *teoría pura del derecho* es la autonomización del Derecho, Política, Sociología, Moral e Ideología. (Kelsen, 1982)

Esta autonomización busca otorgar al Derecho el rango de unidad y carácter científico. Kelsen en su *teoría pura del derecho*, opone el positivismo jurídico o iuspositivismo con el Derecho Natural. (Kelsen, 1993)

En ese sentido, Kelsen sustenta un ordenamiento jurídico sobre la base de la jerarquía normativa donde toda norma obtiene su vigencia de una norma superior. Esta jerarquía tiene su máxima representante en la *Constitución*; sin embargo, ésta tiene aún un sustento anterior conocido como norma fundante básica; La *norma fundante básica* es la fuente común de validez de todas las normas pertenecientes a uno y el mismo orden. Que una norma determinada pertenezca a un orden determinado se basa en que su último fundamento de validez lo constituye la norma fundante básica de ese orden. (Condomi, 2020)

Analizando la estructura de los sistemas jurídicos, puede concluirse que toda norma obtiene su vigencia de una norma superior. Al descartar de este modo todo juicio de valor ético o político, la teoría del Derecho se convierte en un análisis lo más exacto posible de la estructura del derecho positivo. (Kelsen, 1982, pág. 134)

Una norma jurídica no vale por tener un contenido determinado; es decir, no vale porque su contenido pueda inferirse, mediante un argumento deductivo lógico, de una norma fundamental básica presupuesta, sino por haber sido producida de determinada manera, y en última instancia, por haber sido producida de la manera determinada por una norma fundante básica presupuesta. Por ello, y sólo por ello, pertenece la norma al orden jurídico. (Kelsen, 1993, pág. 205)

El Bloque de Constitucionalidad referente a la jerarquía de la Constitución se encuentra el Articulo 410 parágrafo (II) de la Constitución política del Estado de Bolivia:

La Constitución es la norma suprema del ordenamiento jurídico boliviano y goza de primacía frente a cualquier otra disposición normativa. El bloque de constitucionalidad está integrado por los Tratados y Convenios internacionales en materia de Derechos Humanos y las normas de Derecho Comunitario, ratificados por el país. La aplicación de las normas jurídicas se regirá por la siguiente jerarquía, de acuerdo a las competencias de las entidades territoriales:

1. Constitución Política del Estado.
2. Los tratados internacionales.
3. Las leyes nacionales, los estatutos autonómicos, las cartas orgánicas y el resto de legislación departamental, municipal e indígena.
4. Los decretos, reglamentos y demás resoluciones emanadas de los órganos ejecutivos correspondientes.

En consecuencia, la Constitución Política del Estado es la Ley Suprema del Ordenamiento Jurídico Nacional y ninguna disposición de menor rango puede ser contraria a la misma.

La Acción de Protección de Privacidad, es un recurso de última ratio, de última instancia, que puede ser interpuesto cuando se utilizan indebidamente los datos, información, derechos o garantías constitucionales de las personas por medios electrónicos; se encuentra tipificada en el Artículo 130 de la Constitución Política del Estado de Bolivia.

El gran avance de las TIC ha rebasado los límites del derecho positivo, es decir, actualmente no existen normas legales que satisfacen las actividades tecnológicas; es por ello, que la sabiduría de la Constitución Política del Estado ha incorporado el capítulo de *Ciencia, Tecnología e Investigación*, otorgando a las Universidades el desarrollo de los procesos de investigación científica.

Otro importante instituto constitucional, tiene que ver con los derechos y garantías de las personas, entre ellos, el derecho a la privacidad e intimidad y acceso a la información.

El derecho a la Privacidad e Intimidad es una garantía constitucional que no puede ser violentada y menos vulnerada porqué así lo ha dispuesto la Constitución Política del Estado; sin embargo, surge cuestionar el alcance y límite de estas garantías constitucionales en materia de Tecnologías de la Información y Comunicación.

Actualmente, existen millones de recursos informáticos en el *Internet* destinados a capturar y recolectar los datos de las personas naturales y jurídicas para lograr potencializar los bancos de datos de las personas, utilizando medios o herramientas insospechadas e inimaginables para este fin, a modo de ejemplo, cuando una persona se acerca a una entidad financiera y proporciona su número de cédula de identidad, la entidad financiera edita información de la persona hasta el más mínimo detalle o peor aun cuando en las redes sociales se editan datos personalísimos, en muchos casos contenido sexual.

La Ley 1768 del Código Penal 1997 que modifico e insertó el Capítulo XI denominado *Delitos Informáticos* cuyo articulado está compuesto por dos que son los siguientes:

Artículo 363 bis.- Manipulación Informática.- El que con la intención de obtener un beneficio indebido para sí o un tercero, manipule un procesamiento o transferencia de datos informáticos que conduzca a un resultado incorrecto o evite un proceso tal cuyo resultado habría sido correcto, ocasionando de esta manera una transferencia patrimonial en perjuicio de tercero, será sancionado con reclusión de uno a cinco años y con multa de sesenta a doscientos días.

Podemos reflejar de manera simple una manipulación informática:

Si ***a = 3*** y ***b = 4*** entonces ***c = 7***

En el caso de que se presente una manipulación informática tanto a, b o c serán modificados de manera que el proceso generará un dato incorrecto que determinará una transferencia patrimonial en perjuicio de tercero.

Finalmente:

Artículo 363 ter.- Alteración, Acceso y Uso Indebido De Datos Informáticos.- El que sin estar autorizado se apodere, acceda, utilice, modifique, suprima o inutilice, datos almacenados en una computadora o en cualquier soporte informático, ocasionando perjuicio al titular de la información, será sancionado con prestación de trabajo hasta un año o multa hasta doscientos días.

Este tipo penal, tiene que ver esencialmente con el acceso indebido a los dominios de las Tecnologías de la Información, es decir, que alguna persona acceda a los dominios informáticos sin estar autenticado o no tenga permiso de ingreso mediante *login* y *password*.

Otros Tipos Penales.

Dentro de la legislación penal boliviana, existen también otros tipos que se encuadran a los delitos en Tecnologías de la Información y Comunicación , en sentido, que el actuar delincuencial puede ser producido por cualquier medio; Los artículos 281 quater *Difusión e Incitación al Racismo o a la Discriminación*; 281 octies *Insultos y otras Agresiones Verbales por motivos racistas*; 283 *Calumnia*; 285 *Propalación de Ofensas*; 287 *Injuria*; 300 *Violación de la Correspondencia y Papeles Privados*; 312 quater *Acoso Sexual*; 318 *Corrupción de Menores*; 320 *Corrupción de Mayores*; 323 bis *Pornografía de Niñas, Niños o Adolescentes y de Personas Incapaces*; 339 *Destrucción de Cosas Propias Para Defraudar*.

1.5.3 **Justificación Técnica.**

La presente investigación se justifica técnicamente porque es desarrollada en base a requerimientos y necesidades recurrentes en el proceso de investigación de las acciones antijurídicas en el entorno de las TIC; considerándose, que en estas necesidades se deben tomar recaudos sobre la *Cadena De Custodia* y evitar la contaminación de la *Evidencia Digital* en la recolección, análisis e interpretación de

la misma.

Técnicamente se hará uso de las siguientes áreas:

- Tecnologías de la Información y Comunicación: será la base que permitirá establecer la capacidad del conocimiento humano, su desarrollo e interacción con los modelos matemáticos;
- Sistemas de Información: será la base para conceptualizar los componentes, acciones, alcance y confiabilidad de los procesos inherentes a las Tecnologías de la Información;
- Derecho Informático: será la base por cual se plantearán definiciones sobre la interrelación entre el Derecho y la Informática forense.
- Delitos Informáticos: será la base para establecer las acciones antijurídicas en el entorno de las Tecnologías de la Información;
- Evidencia Digital: será la base para la construcción de campos magnéticos y pulsos electrónicos que pueden ser recolectados, almacenados y analizados con herramientas técnicas especiales, en este caso, con modelos matemáticos.
- Cadena de Custodia Digital: será la base que deberá adoptarse con el fin de preservar la identidad e integridad de la evidencia digital como fuente del valor probatorio para los delitos informáticos, para su eficacia procesal.
- Algoritmos matemáticos, Modelo Matemático o modelo científico en ciencias aplicadas: será la base para expresar relaciones, proposiciones sustantivas de hechos, variables, parámetros, entidades y relaciones entre variables de las operaciones, para estudiar, analizar e interpretar comportamientos de las Tecnologías de la Información y Comunicación.

1.6 **Objetivos.**

1.6.1 **Objetivo General.**

Proponer **LINEAMIENTOS JURIDICOS PARA LA INCLUSION DEL USO ALGORITMICO EN EL PROCESO EN LA BUSQUEDA DE LA EVIDENCIA DIGITAL** para colaborar a la actualización del ordenamiento jurídico boliviano de manera que se mejoren las probabilidades de la averiguación de la verdad material en las acciones antijurídicas en las Tecnologías de la Información y Comunicación.

1.6.2 **Objetivos Específicos.**

1. Estudiar la legislación comparada acerca del tratamiento y regulación de los Delitos Informáticos y la Evidencia Digital;
2. Analizar los Acuerdos y Tratados Internacionales relacionados con los delitos informáticos y la evidencia digital.
3. Exponer la necesidad de incluir el uso algorítmico en la búsqueda de la Evidencia Digital como prueba irrefutable para la averiguación de la verdad material en acciones antijurídicas en las Tecnologías de la información y Comunicación.

1.7 **Hipótesis**.

Con la proposición de lineamientos jurídicos para la inclusión del uso algorítmico en el proceso de la búsqueda de la evidencia digital se colaborará con la actualización del ordenamiento jurídico boliviano de manera que se mejoren las probabilidades de la averiguación de la verdad material en las acciones antijurídicas en las Tecnologías de la Información y Comunicación.

1.8 **Metodología de la Investigación**

La metodología se constituye la médula del plan; se refiere a la construcción de las unidades de análisis o de investigación, las técnicas de observación y recolección de datos, los instrumentos, los procedimientos y las técnicas de análisis (Ibañez, 2003).

De esta forma se efectuó un análisis de la ley y otras disposiciones legales para el uso algorítmico en el proceso de búsqueda de la *Evidencia Digital* en las acciones antijurídicas en las TIC.

En cualquier campo de actividad, el método es el medio para alcanzar el propósito determinado. Como es de saber es el fin de toda ciencia, el método científico en general es el modo de proceder para obtener conocimientos, es una disciplina que estudia el Derecho, para tener nivel científico, tendría que ser metódica. Las etapas del método científico según Francisco Romero distribuyen las etapas del método científico, según el método, en: a) Investigación, b) Sistematización, y c) Comunicación.

a) En la investigación, el investigador toma contacto directo con aquello que es objeto de su ciencia, para descubrir nuevos entes, nuevas substancias, nuevos fenómenos y también, para sorprender entre ellos relaciones distintas a las ya conocidas, como no existentes;
b) En la sistematización se ordenan los nuevos conocimientos adquiridos mediante la investigación, asignándole el lugar que les corresponde dentro del marco de la ciencia. Es decir, se los coordina, subordina y supraordinada con otros conocimientos previamente logrados, en un conjunto jerarquizado, consistente y perspicuo;
c) La comunicación dispone los conocimientos ya sistematizados en un orden adecuado para su transmisión a otras personas; (Moscoso, 2008)

La metodología aplicable en la presente investigación será a través de los métodos de investigación dogmático jurídico, sociológico jurídico, legislativo comparativo, inductivo, deductivo y científico.

1.8.1 **Método Dogmático – Jurídico.**

El método empleado en el estudio fue el dogmático–jurídico, porque se realizó un análisis del derecho positivo vigente comparado e internacional describiendo y determinando el alcance de las leyes con relación al tema específico. Este método constituye el orden jurídico, es decir, lo investigado es la norma jurídica en su contenido dispositivo abstracto, su fin es la determinación del contenido normativo del orden jurídico (Witker, 1999)

1.8.2 **Método Inductivo.**

El método inductivo es aquel método científico que obtiene conclusiones generales a partir de premisas particulares. Se trata del método científico más usual, en el que pueden distinguirse cuatro pasos esenciales: la observación de los hechos para su registro, la clasificación y el estudio de estos hechos, la derivación inductiva que parte de los hechos y permite llegar a una generalización y la contrastación.

El método Inductivo es necesario en la presente investigación ya que la generalización de los eventos es un proceso que sirve para la estructuración de todas las ciencias, que se basan en la observación de un fenómeno y posteriormente se realizan investigaciones y experimentos que conducen esta generalización, lo que se realiza implícitamente en la investigación presente.

1.8.3 **Método Deductivo.**

En el método deductivo, se suele decir que se pasa de lo general a lo particular, de forma que partiendo de unos enunciados de carácter universal y utilizando instrumentos científicos, se infieren enunciados particulares, pudiendo ser axiomático-deductivo, cuando las premisas de partida están constituidas por axiomas, es decir, proporciones no demostrables, o hipotéticos-deductivo, si las premisas de partida son hipótesis contrastables (Mandamiento Ortiz, Arturo; Ruiz Aponte, Domingo, 2017)

Este método es necesario para la presente investigación ya que mientras las proposiciones del método Inductivo son concreciones que establecen como son los fenómenos, sus causas y efectos reales, los del método deductivo son premisas que tratan de establecer lo significativo de los fenómenos según el raciocinio del investigador, lo cual termina de aplicarse en la demostración de la hipótesis, técnicas e instrumentos.

- Documental. Para el estudio de la presente investigación científica se toman diferentes fuentes, como ser: Constitución Política del Estado, Código Penal, Código de Procedimiento Penal, Ley del Ministerio Público, Reglamentos de la Fuerza Especial de Lucha Contra el Crimen; además de Legislaciones de otros países.
- Revisión de bibliografía especializada. Se utilizaron libros especializados en la materia de Derecho Procesal Penal y sobre Delitos Informáticos para dar una explicación doctrinal del problema, y de la misma manera demostrar su importancia.
- Entrevista. La entrevista es una …*comunicación interpersonal… que se produce entre el investigador y el sujeto de estudio, para obtener respuestas verbales a las interrogantes planteadas sobre el problema propuesto* (Koria, 2007).

La entrevista, consiste en la recepción en que el entrevistado proporciona información directa al investigador, además en una relación personal, a través de esta interacción del entrevistado, se obtienen datos e información sobre elementos que el individuo no escribiría nunca y que son imposibles de observar directamente. (Zegarra, 2002)

CAPÍTULO 2

LEGISLACIÓN COMPARADA ACERCA DE LOS DELITOS INFORMÁTICOS Y EL PROTOCOLO DE LA EVIDENCIA DIGITAL.

2.1 Introducción

En el presente capítulo se comenzará con un conjunto de conceptualizaciones y caracterizaciones esenciales para poder comprender las posteriores redacciones encontradas en el estudio de legislación comparada. Posteriormente se pasará al análisis de la normativa de países escogidos en función a su especialización en la temática para terminar con un análisis de la legislación boliviana. Esto pondrá en evidencia la carencia de redacción específica en las normas penales sustantivas y adjetivas del sistema boliviano, así como la carencia de un protocolo específico para el tratamiento de la evidencia digital.

2.2 El Delito Informático

Nidia Callegari lo define como aquel que se da con la ayuda de la informática o de técnicas anexas.

Julio Téllez lo define como las conductas típicas, antijuridicas y culpables en que se tiene a las computadoras como instrumento o fin y por las segundas; actitudes ilícitas en que se tienen a las computadoras como instrumento o fin. (Acurio Del Pino, 2016)

Por otro lado, el Convenio de Ciberdelincuencia del Consejo de Europa en llevado a cabo en Hungría, Budapest, 2001, el cual fue puesto en vigencia el año 2004; los define como: Actos que amenazan la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, así como el abuso de dichos sistemas, medios y datos. (Organización de los Estados Americanos, 2001)

Las actuales condiciones tecnológicas, hacen totalmente necesaria la incorporación de valores inmateriales en las Tecnologías de la Información y Comunicación como bienes jurídicos de protección, esto tomando en cuenta las diferencias existentes por ejemplo entre

la propiedad tangible y la intangible. Esto por cuanto la información no puede ser tratada de la misma forma en que se aplica la legislación actual a los bienes corporales. (Acurio Del Pino, 2016)

2.3 Bien Jurídico en las Tecnologías de Información y Comunicación

Al constituirse las Tecnologías de la Información y Comunicación en un bien jurídico protegido por la esfera del Derecho, esta debe ser considerada en diferentes formas, ya sea como un valor económico, como uno valor intrínseco de la persona, por su fluidez y trato jurídico, y finalmente por los sistemas que la procesan o automatizan; los mismos que se equiparan a los bienes jurídicos protegidos tradicionales, según Acurio del Pino, tales como:

- **El Patrimonio**, en el caso de la amplia gama de fraudes informáticos y las manipulaciones de datos que dañan el patrimonio de las personas naturales y personas jurídicas;
- **La Reserva, la Intimidad y Confidencialidad de los Datos**, en el caso de las agresiones informáticas a la esfera de la intimidad en forma general, especialmente en el caso de los bancos de datos o la publicación de fotos y videos privados con contenido explícito de tipo sexual;
- **La Seguridad o Fiabilidad del Trato Jurídico y Probatorio**, en el caso de falsificaciones de datos o documentos probatorios vía medios informáticos o electrónicos;
- **El Derecho de Propiedad**, en este caso sobre la información o sobre los elementos físicos, materiales de un sistema informático. (Acurio Del Pino, 2016, p. 21)

Por tanto, se puede resumir que el bien jurídico protegido, acoge a la confidencialidad, integridad, disponibilidad de la información y de los sistemas informáticos donde esta se almacena o se transfiere información.

Los autores chilenos Claudio Magliona y Macarena López manifiestan que, sin embargo, los delitos informáticos tienen el carácter de pluriofensivos o complejos, es decir …*que se caracterizan porque simultáneamente protegen varios intereses jurídicos, sin perjuicio de que uno de tales bienes está independientemente tutelado por otro tipo*.

Asimismo, la delincuencia informática puede afectar a bienes jurídicos tradicionalmente protegidos por el ordenamiento penal, tal el caso de delitos contra la moral, el honor y la privacidad de las personas, en los que se utiliza el computador y el Internet para publicar fotos y videos difamando a personas físicas naturales; o de otra manera atentar contra la integridad personal, la fe pública o la seguridad nacional. Cabe mencionar, que en otros casos las conductas del agente van dirigidas a lesionar bienes no protegidos tradicionalmente por la legislación penal, tal el caso de los bienes Informáticos, consistentes en datos, información computarizada, archivos y programas insertos en el soporte lógico del ordenador. (Acurio Del Pino, 2016, p. 8)

2.4 **La Evidencia Digital.**

Por Evidencia Digital se entiende al conjunto de datos en formato binario, que comprende los ficheros, su contenido o referencias a éstos meta-datos que se encuentren en los soportes físicos o lógicos del sistema atacado (López, 2007).

La *Evidencia Digital* es un término utilizado de manera amplia para describir cualquier registro generado o almacenado en un sistema computacional que puedan ser utilizados como pruebas en un proceso legal. (EIIDI, 2012)

Acurio del Pino:

> La *Evidencia Digital*, debe mantenerse totalmente integra dentro del proceso de investigación para que esta tenga validez jurídica.
>
> La *Evidencia Digital* describe cualquier registro generado por o almacenado en un sistema computacional que puede ser utilizado como prueba en un proceso legal, la misma se divide en tres categorías:
>
> - Los registros almacenados en el equipo electrónico (por ejemplo, correo

electrónico, archivos de aplicaciones de ofimática, imágenes, etc.);

- Los registros generados por los equipos electrónicos (por ejemplo, registros de auditoría, registros de transacciones, registros de eventos, etc.);
- Los registros que parcialmente han sido generados y almacenados en los equipos electrónicos (hojas de cálculo financieras, consultas especializadas en bases de datos, etc.). (Acurio Del Pino, 2014)

2.4.1. Características de la Evidencia Digital

La *Evidencia Digital* se constituye como la *prueba del delito* para los investigadores forenses durante un proceso de investigación por lo cual, es preciso detallar alguna de las características propias de dicha evidencia:

- Es volátil;
- Es anónima;
- Es duplicable;
- Es alterable y modificable;
- Es eliminable.

Las características de la evidencia digital implican que el investigador debe tener conocimientos tanto en procedimientos, técnicas y herramientas tecnológicas para obtener, custodiar, revisar, analizar y presentar la misma en estrados judiciales. (Acurio Del Pino, Manual de manejo de evidencias digitales y entornos informaticos, 2014)

2.5 Algoritmo Matemático.

El algoritmo según la RAE quizá del latín tardío algobarismus, y este abrev. del ár. cl ás. ḥisābu lgubār cálculo mediante cifras arábigas, se refiere a un conjunto sistémico de instrucciones, pasos y reglas definidas y limitadas, para dar lugar a un resultado.

Según la Real Academia Española se trata de un conjunto ordenado y finito de operaciones que permite hallar la solución de un problema. (RAE, 2022)

Implica una serie de operaciones no ambiguas para ejecutarse paso a paso que conducen a un resultado y se representa mediante una herramienta o técnica. Se trata de un procedimiento lógico formal: Problema (Entrada) y Solución (Salida) en un Procesamiento.

Como categoría propia de las matemáticas e informática y pese a la falta de una uniforme concepción, han resultado admisibles tres características de los algoritmos:

- Debe ser preciso e indicar el orden de realización de cada paso,
- Debe ser definido; si se sigue un algoritmo dos veces, se debe obtener el mismo resultado cada vez,
- Debe ser finito, si se sigue un algoritmo se debe terminar en algún momento; o sea debe tener un número finito de pasos.

También dependen de formas de expresión que van desde el lenguaje natural, diagramas de flujo hasta seudocódigos y el lenguaje de programación. No obstante, el lenguaje natural o común adolece de problemas semánticos, por lo que en materia de informática se emplean los otros métodos. (Takeyas, 2019)

Ciencia Forense.

La ciencia forense es la aplicación de prácticas científicas dentro del proceso legal. El proceso de investigación es desarrollado por investigadores altamente especializados o criminalistas que localizan evidencias en lugar del hecho. Parte de la evidencia que hallan a menudo no puede ser vista a simple vista, a veces es hasta más pequeña. La ciencia forense ahora usa de manera rutinaria ADN en delitos seriamente complejos. (Orta, 2023)

La ciencia forense proporciona a los investigadores, principios y técnicas que facilitan la investigación del delito criminal para identificar, recuperar, reconstruir o analizar la evidencia durante una investigación criminal forma parte de la ciencia forense. (Franciéllen

de Barros; Barbara Kuhnen; Mônica da Costa Serra; Clemente Maia da Silva Fernandes, 2020)

Los principios científicos que se emplean en el procesamiento de una evidencia son reconocidos y usados en procedimientos como:

- Recoger y examinar huellas dactilares y ADN;
- Recuperar documentos de un dispositivo dañado;
- Hacer una copia exacta de una evidencia digital;
- Generar una huella digital con un algoritmo hash MD5 o SHA1 de un texto para asegurar que éste no se ha modificado;
- Firmar digitalmente un documento para poder afirmar que es auténtico y preservar la cadena de custodia de la evidencia digital.

Un principio fundamental en la ciencia forense para relacionar un criminal con el crimen que ha cometido es el *Principio de Intercambio* o Transferencia de Edmond Locard un francés fundador del instituto de criminalística de la Universidad de Lyon. Este principio fundamental sostiene que todo contacto deja un rastro. Es decir que cualquiera o cualquier objeto que entra en la escena del crimen deja un rastro en el lugar del hecho o en la víctima y viceversa. (Garcia Collantes, 2018)

2.6 **Cadena de Custodia Digital.**

La cadena de custodia digital es el procedimiento que permite de manera inequívoca conocer la identidad, integridad y autenticidad de los vestigios o indicios digitales relacionados con un acto delictivo, desde que son encontrados hasta que se aportan al proceso judicial como pruebas.

La importancia de preservar correctamente la cadena de custodia digital, debido a las especiales características de las evidencias digitales, radica en el hecho de poder garantizar el uso de éstas como prueba.

La *Cadena De Custodia Digital* garantiza la fiabilidad de la prueba digital que se aporta en el juicio y la adecuada defensa mediante la correspondiente pericial informática. Resulta imprescindible dentro del procedimiento de prueba pericial informática/tecnológica, para garantizar su autenticidad e integridad, debido a que puede ser fácilmente manipulada.

Si el proceso de obtención de la evidencia digital es el preciso se consigue evitar la contaminación de los medios probatorios. Es importante que al localizar el material objeto de investigación se documente y fotografíe la obtención de la prueba digital discos duros, dispositivos móviles, portátiles, aplicaciones y otros. (LISA Instituto., 2023)

Una vez que han sido desarrollados estos conceptos y ejemplos importantes para comprender el lenguaje manejado por la legislación especializada en delitos informático y evidencia digital se puede pasar al estudio legislativo propuesto en el presente objetivo de investigación.

A continuación, se estudiarán algunas de las legislaciones más importantes respecto a el *Delito Informático,* la *Evidencia Digital* y *Cadena de Custodia Digital*.

2.7 Estudio de caso. Países con gran desarrollo de normas y protocolos para los delitos informáticos y el tratamiento de la evidencia digital.

2.7.1 Estados Unidos de América

Estados Unidos de América tiene la legislación más completa en materia de delito informático y cibernético o cibercrimen.

El primer abuso de la computadora se registró en 1958 pero no fue hasta 1966 que se llevó adelante el primer proceso por la alteración de datos de un Banco de Minneapolis.

En la primera década de los 70, mientras los criminólogos y especialistas de informática debatían y discutían si el Delito Informático era el resultado de una nueva tecnología, los ataques se hicieron más frecuentes, hacia el Pentágono, la Organización del Tratado del Atlántico Norte (OTAN), las universidades, la Administración Nacional de Aeronáutica y el Espacio NASA, los laboratorios industriales y militares se convirtieron en el blanco de los intrusos.

En 1994 la legislación norte americana adoptó el Acta Federal de Abusos Computacionales Sección 18 U.S. Artículo 1030 que modifica el Acta de 1986: El modificar, destruir, copiar, trasmitir datos o alterar la operación normal de las computadoras, los sistemas o las redes informática, es un delito.

Federal Computers Investigation Committe (FCIC) es la organización más importante e influyente en relación a los *Delitos Informáticos*: Los investigadores estatales y locales, auditores financieros, agentes federales, abogados, policías, programadores trabajan allí comunitariamente. (Christy, 1980)

Además, existe la Asociación Internacional de Especialistas en Investigación Computacional (IACIS), que investiga nuevas técnicas para dividir los sistemas sin destruir las evidencias. Sus integrantes, son forenses informáticos y trabajan además de en EEUU, Canadá, Taiwán e Irlanda. (IACIS, 2022)

Para estudiar ésta legislación respecto del llamado Cibercrimen y en general de cualquier otra materia, es necesario tener presente dos características estructurales:

Lo primero, es que pertenece a la tradición del Common Law *Ley Común,* por lo que además de las reglas emanadas de las leyes en sentido estricto statutes *Actas,* existen normas jurídicas que emanan del derecho consuetudinario o común heredado originalmente de la Corona Inglesa, y luego desarrollado e interpretado por los jueces. (Godoy F, 2019)

Por otra parte, la organización del Estado es federativa, lo cual implica que cada Estado es parte de la Unión. Es decir que cada Estado dicta y aplica sus propias leyes y regulaciones, sin perjuicio de la obligación de respetar la Constitución Federal y, particularmente, de respetar el ámbito de competencia que aquella atribuye al gobierno federal. De hecho, su legislación ha jugado un rol muy significativo en la persecución de delitos informáticos como el fraude y acceso ilegal trespass, cuyo origen está en la jurisprudencia del common law. En 1984 se dictó la Ley de fraude, acceso ilegal y vandalismo Informático. (Meza-Lopehandia, 2014)

El Delito Cibernético o cybercrime, se refiere a todo delito en el cual está presente un elemento informático. (Meza-Lopehandia, 2014) Y, Delito Informático o Ciberdelito este describe aquellas conductas ilícitas que tienen por objeto un sistema informático. (Mayer Lux, 2017)

El cibercrimen o delitos cibernéticos en el sentido amplio, abarca tanto delitos comunes que se ejecutan a través de medios informáticos, como nuevos delitos, cuya ejecución sólo es posible gracias a la existencia de dichos medios. La respuesta a este tipo de criminalidad apela tanto a la legislación general como a leyes especialmente diseñadas para combatirla, sin perjuicio de que se critique la inadecuación de la

legislación basada en la jurisdicción estatal para perseguir un fenómeno de alcance global. (Meza-Lopehandia, 2014, p. 3)

Los Delitos Informáticos se dividen en seis grupos: fraude y acceso ilegal, terrorismo, obscenidades, copyright, difamación y amenazas y acoso cibernético.

- **Fraude y acceso ilegal**.- Esta normativa federal tipificó siete conductas relativas a acceso ilegal a computadoras, aunque sólo se refiere a "ordenadores protegidos", esto es, aquellos utilizados por instituciones financieras, el gobierno federal, o usados en comercio o comunicaciones entre estados de la Unión o terceros Estados. Ahora bien, la noción de ordenadores protegidos es suficientemente amplia como para comprender todo computador conectado a Internet, pues incluye aquellos utilizados para la comunicación interestatal. (Meza-Lopehandía, 2014)

Se refiere a la suplantación de identidad y la utilización fraudulenta de dispositivos de acceso a redes informáticas o bases de datos como:

  - **Usurpación de identidad**. La expresión hurto de identidad podría ser empleada para describir el robo o la usurpación de una identidad existente o de una parte importante de la misma, con o sin consentimiento, independientemente de que la víctima esté viva o muerta. Esta definición también contiene dos elementos: el objeto la identidad y el acto correspondiente la usurpación. En consecuencia, no abarca la transferencia de información relativa a la identidad ni la utilización de dicha información. (Gercke, 2007)
  - **Fraude y Dispositivos de Acceso**. La Ley Federal considera como delito actividades que utilicen de un modo ilegítimo dispositivos de acceso tales como: tarjetas, códigos, números seriales y contraseñas, para obtener dinero, bienes, servicios u otros valores de modo fraudulento.

La Ley USA Patriot, dictada en 2001 como reacción a la amenaza terrorista, extendió la aplicación de esta ley más allá de la jurisdicción de los EE.UU, siempre que la comisión del delito incluyere un dispositivo emitido en el país y que el imputado hubiere transportado, enviado o almacenado en dicho país algún elemento para cometer el delito. (Meza-Lopehandía, 2014)

- **Terrorismo.**- La Ley USA Patriot, incorpora los delitos mencionados en articulo 1.030 US Code a la definición de delito criminal de terrorismo, cuando se dan los presupuestos legales para ello, o sea, cuando la actividad fraudulenta se lleva a cabo en el marco de actividad terrorista doméstica o

internacional, de acuerdo a la definición provista por la sección 2331 del título 18 del US Code. (Meza-Lopehandía, 2014)

La Ley Patriota de los Estados Unidos es un acrónimo de Unir y Fortalecer América al Proporcionar las Herramientas necesarias para Interceptar y Obstruir el Terrorismo (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism) (Lecours, 2007)

- **Fraude y actividad relacionada en relación con las computadoras**: El fraude informático suele relacionarse con el phishing y —en menor medida— con el pharming. En la práctica, este último se vincula con la ejecución de operaciones bancarias, cuya verificación en línea constituye un ámbito idóneo para manipular o alterar datos o programas de sistemas informáticos, a fin de perjudicar el patrimonio de terceros. (Mayer, Laura ; Calderon, Guillermo, 2020, p. 157)

- **Obscenidades**.- Este tipo de delito se refiere a la producción de material obsceno o indecente con el ánimo de comercializarlo o distribuirlo, incluyendo Internet, está prohibida en los EE.UU. Sin perjuicio de ello, la Corte Suprema ha protegido la producción y distribución de pornografía a través de la libertad de expresión de la Primera Enmienda, siempre y cuando no constituya obscenidad.; (Acurio Del Pino, 2016)

  - **Pornografía infantil**.- La pornografía infantil está prohibida, y las penas asociadas van desde cinco a cuarenta años de presidio. A este respecto, la Corte Suprema ha declarado que esta prohibición no alcanza a la pornografía infantil virtual y ha declarado inconstitucionales la prohibición contenida en esta materia en la Ley de Prevención de la Pornografía Infantil de 1996 (CPPA). Más tarde, con la entrada en vigor de la Ley Protect de 2003; Ley de Protección se logró prohibir la pornografía infantil virtual, al incluir el requisito de obscenidad del material prohibido, aunque persisten las dudas de constitucionalidad.
  - **Prohibición de dominios engañosos.-** El artículo 2.252(B) de la Sección 18 del US Code sobre crímenes y procedimiento criminal castiga con hasta diez años de cárcel la utilización de dominios de Internet con nombres engañosos que lleven al usuario a ver material obsceno. Las palabras porn y sex nunca pueden ser consideradas engañosas. (Acurio Del Pino, 2016)

- **Prohibición de uso de recursos públicos para adquisición de ordenadores sin filtros**.- La Ley de Protección de los Niños de Internet (CIPA), prohíbe a las bibliotecas públicas la adquisición de ordenadores con acceso a Internet, salvo cuando cuenten con tecnología que permita filtrar contenido inapropiado para menores. (Acurio Del Pino, 2016)
- **Seducción de menores para propósitos sexuales**.- Articulo 2.425 de la sección 18 del US. Code criminaliza el uso del correo o el comercio para transmitir información destinada a solicitar favores sexuales a un menor. Esta norma se utiliza para perseguir a los pedófilos que utilizan Internet para seducir a menores. (Acurio Del Pino, 2016)

- **Protección de Copyright**: En general, quien alegue infracción a sus derechos de copyright debe probar: Propiedad de un copyright válido; Copia (una); Apropiación indebida de un tercero.

  El acusado puede defenderse probando que su copia contiene una creación original o, más usualmente, puede ampararse en el uso justo fair use. (Meza-Lopehandía, 2014)

  La Ley NET de 1998 y la Ley de Copyright del Milenio Digital (DMCA), que se dictaron como reacción al fenómeno de compartición de archivos por Internet, intentaron permitir la prosecución de las infracciones al copyright, aún sin ánimo de lucro, pero su uso ha continuado siendo escaso. (Meza-Lopehandía, 2014)

  - **Difamación**: No existe normativa federal en esta materia, por lo que sólo se regula a nivel estadual y de Common Law. Éste último distingue entre quienes publican primary publishers, los distribuidores y los portadores (tales como una compañía de teléfonos), siendo los primeros los principales responsables por eventuales actos difamatorios, y los últimos, los que no tienen responsabilidad. (Meza-Lopehandía, 2014)
  - **Amenazas y acoso cibernético**: La sección 2.261A del título 18 del US Code tipifica el uso de correo o el comercio interestatal o internacional para amenazar a una persona o a familia con la muerte o serias lesiones físicas. Esta disposición se ha utilizado para perseguir amenazas serias y verosímiles vertidas a través de Internet, en tanto éste constituye un medio de comercio interestatal. (Meza-Lopehandía, 2014)

Evidencia Digital y su tratamiento.

En delitos en contra de los derechos fundamentales de la persona está bajo la custodia y cumplimiento de los protocolos de la Informática Forense de la Brigada de Investigación Criminal. Federal Bureau of Investigation (FBI) en su Unidad del Crimen Computacional (Computer Crime Unit) y otros organismos. Así de la misma manera se encuentra el Comité Federal de Investigación Computacionales (FCIC) el Centro de Estudios Estratégicos e Internacionales (CSSI), la Asociación Internacional de Especialistas en Investigación Computacional (IACIS) Utilización de Informática Forense (UIF). (Meza-Lopehandía, 2014)

La Brigada de Investigación Criminal (FBI) tiene competencias respecto a lo siguiente:

La adquisición: es la recolección efectiva del objeto de estudio o elemento de análisis;

La preservación: el mantenimiento de dicho elemento de examen a peritar en su estado original, evitando su alteración en lo más mínimo que pueda brindar un resultado erróneo;

La obtención: es la observación en sí, determinándose que la información es efectivamente la que se desea indagar. Siendo los casos más normales, como para ejemplificar, el chequeo de historial de navegación, recuperación de archivos de texto o imágenes borrados de forma poco segura, entre otros procedimientos. Y finalmente;

La presentación: la cual hace referencia a la exposición de un informe utilizando un lenguaje acorde a quienes sean los destinatarios del análisis. Dado que, tanto las partes como el juez son los principales ingresados de los resultados de esta actividad pericial.

El ISFS, Information Security and Forensic Society - Hong Kong(Sociedad de Seguridad Informática y Forense, Guía Hong Kong) , publicó Computación Forense - Parte 2: Mejores Prácticas. La guía Hong Kong cubre los procedimientos y otros requerimientos necesarios involucrados en el proceso forense de evidencia digital, desde el examen de la escena del crimen hasta la presentación de los reportes en la Corte. (Yañez, 2020)

Su estructura es:

- Introducción a la computación forense.
- Calidad en la computación forense.
- Evidencia digital.
- Recolección de Evidencia.
- Consideraciones legales Hong Kong.

Esta guía cubre los procedimientos y requerimientos necesarios involucrados en el proceso forense de la *Evidencia Digital*, desde el examen de la escena del crimen hasta la presentación de los reportes en la Corte. (Yañez, 2020)

Digital Forensic Process. El uso de estándares como en toda investigación; la ciencia forense informática en EEUU cuenta con las siguientes fases:

- Fase de Adquisición de la evidencia digital
- Fase de Autenticación de la evidencia digital
- Fase de Análisis de la evidencia digital.

El departamento de defensa de EEUU utiliza otros estándares más como:

- Fase para estandarizar formatos de los datos forenses
- Se debe incluir técnicas
- Se deben aplicar metodologías de conformidad, la cual tiene especial interés en la interoperabilidad con otros organismos.

El Proceso Integrado de Investigación Digital (IDIP) se basa en investigación en el que se considera a la computadora la escena del crimen.

- Preparación
- Despliegue
- Investigación de la escena física
- Investigación de la escena digital
- Presentación de conclusiones (3Ciencias, 2020, p. 23)

2.7.2 **Reino de España.**

La legislación española en relación a los *Delitos Informáticos* cuenta con un abanico de leyes a continuación, se citan las más relevantes:

La Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPD-GDD) es una ley orgánica aprobada por las Cortes Generales de España que tiene por objeto adaptar el Derecho interno español al Reglamento General de Protección de Datos de la Unión Europea (BOE-A-2018-16673, 2018).

Se sanciona en forma detallada la obtención o violación de secretos, el espionaje, la divulgación de datos privados, las estafas electrónicas, el hacking maligno o militar, el pirateo telefónico *phreacking* y la introducción de virus. Aplicando pena de prisión y multa, agravándolas cuando existe una intención dolosa o cuando el hecho es cometido por parte de funcionarios públicos.

Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.

Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual.

Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.

Real Decreto-ley 7/2022, de 29 de marzo, sobre requisitos para garantizar la seguridad de las redes y servicios de comunicaciones electrónicas de quinta generación.

El Nuevo Código Penal de España describe las siguientes referencias adecuadas al Convenio de Budapest de 2001.

Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos.

El artículo 197 CP contempla las penas con las que se castigará:

A quien, con el fin de descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de cualquier documentación o efecto personal, intercepte sus telecomunicaciones o utilice artificios de escucha, transmisión, grabación o reproducción de cualquier señal de comunicación.

A quien acceda por cualquier medio, utilice o modifique, en perjuicio de terceros, a datos reservados de carácter personal o familiar, registrados o almacenados en cualquier tipo de soporte.

Si se difunden, revelan o ceden a terceros los datos o hechos descubiertos.

En el artículo 278.1 CP se exponen las penas con las que se castigará a quien lleve a cabo las mismas acciones expuestas anteriormente, pero con el fin de descubrir secretos de empresa.

El artículo 264 CP trata de las penas que se impondrán al que por cualquier medio destruya, altere, inutilice o de cualquier otro modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos.

Delitos informáticos

Los artículos 248 y 249 CP tratan de las estafas. En concreto el artículo 248.2 CP considera las estafas llevadas a cabo mediante manipulación informática o artificios semejantes.

Los artículos 255 y 256 CP mencionan las penas que se impondrán a quienes cometan defraudaciones utilizando, entre otros medios, las telecomunicaciones.

Delitos relacionados con el contenido

El artículo 186 CP cita las penas que se impondrán a aquellos, que, por cualquier medio directo, vendan, difundan o exhiban material pornográfico entre menores de edad o personas con discapacidad necesitadas de especial protección.

El artículo 189 CP trata las medidas que se impondrán quien utilice a menores de edad o a personas con discapacidad con fines exhibicionistas o pornográficos, tanto públicos como privados, y quien produzca, venda, distribuya, exhiba o facilite la producción, venta, distribución o exhibición de material pornográfico, en cuya

elaboración se hayan utilizado menores de edad o personas con discapacidad necesitadas de especial protección.

Delitos relacionados con infracciones de la propiedad intelectual y derechos afines

El artículo 270 CP enuncia las penas con las que se castigará a quienes reproduzcan, distribuyan o comuniquen públicamente, una parte o la totalidad, de una obra literaria, artística o científica, con ánimo de obtener un beneficio económico directo o indirecto y en perjuicio de tercero.

El artículo 273 CP trata las penas que se impondrán a quienes, sin consentimiento del titular de una patente, fabrique, importe, posea, utilice, ofrezca o introduzca en el comercio objetos amparados por tales derechos, con fines industriales o comerciales. (Division Forensic Computer, 2022)

Evidencia Digital

La Evidencia Digital es la información o datos, almacenados o transmitidos en formato binario y que han sido determinados a través un proceso de análisis y que sea relevante para la investigación. (UNE Normativa Española, 2022)

En un proceso de investigación penal relacionado a los delitos informáticos y en cuanto a métodos de probatoria y demás tecnicismos legales se puede acudir a la Ley de Enjuiciamiento Criminal y La Nueva Ley de Enjuiciamiento Civil. (López, 2007)

Las normativas utilizadas para la recolección, análisis, interpretación y obtención de evidencias digitales son:

- UNE197010:2015 Es la norma específica para la elaboración de informes y dictámenes periciales sobre las Tecnologías de la información y comunicación

- UNE710505:2013 Es la norma que define el Sistema de Gestión de Evidencias Digitales (SGEE), así como los formatos de intercambio y los mecanismos técnicos aplicables para el mantenimiento de su confiabilidad.
- UNE71506:2013 Es la norma que ha sido elaborada para definir el proceso de análisis forense dentro del ciclo de gestión de las evidencias electrónicas, complementando todos aquellos otros procesos que conforman dicho sistema de gestión de las evidencias digitales.
- ISO/IEC27037:2012 Es la norma orientada al procedimiento de la actuación pericial en el escenario de la recogida, identificación y secuestro de la evidencia digital, no entra en la fase de Análisis de la evidencia.
- ISO/IEC27042:2015 Es la norma que proporciona directrices sobre cómo un perito informático puede abordar el análisis e interpretación de una evidencia digital en un incidente o en una intervención pericial, desde su identificación (evidencia digital potencial), pasando por su análisis (evidencia digital) hasta que es aceptada como prueba en un juicio (evidencia digital legal). (UNE Normativa Española, 2022)

En relación a estas normativas podemos decir que el primero se utiliza para dictámenes e informes periciales respecto de las TIC, el segundo para el vocabulario y principios generales, buenas prácticas de las evidencias electrónicas y las ultimas para el análisis de evidencias informáticas (Romero C, Martha; Choez Ch, Miguel; Alava M, Crhistian; Romero C, Vicente; Castillo M, Miriam; Murillo Q, Leonardo; Delgado L, Holger, 2020)

La legislación española para perseguir un ciberdelito hace uso de la ciencia informática para hallar la evidencia digital que es la prueba digital en este tipo de delitos. La ciencia encargada es la *Informática Forense.*

Miguel López, explica las fases del Análisis Forense Digital:

La primera fase es la *identificación* de la evidencia digital se sigue dos pasos importantes que es la pesquisa y la recolección de evidencias para su posterior fase.

La recopilación de evidencias es la más importante de ambas y la que permite determinar el método de entrada al sistema, la actividad de los intrusos, su identidad y origen, esta fase es la más importante para evitar la contaminación y para evitar alterar las evidencias durante el proceso. Es muy importante documentar cada fase del análisis hasta el final del proceso.

La segunda fase es la *Preservación* de la evidencia en esta fase es imprescindible definir métodos adecuados para el almacenamiento y etiquetado de las evidencias.

Para dar inicio al análisis se deberá hacer una *copia* de la *Recopilación* de Evidencias. Para distinguir de la *Evidencia original* es importante etiquetar y proteger esta última.

La tercera fase es la *Cadena de Custodia* que es en la cual se establecen las responsabilidades y controles de cada una de las personas que manipulen la evidencia. Para ello se deberá preparar un documento en el que se registren los datos personales de todos los implicados en el proceso de manipulación de las copias, desde que se tomaron hasta su almacenamiento.

La cuarta fase es el *Análisis de la Evidencia:* Una vez que disponemos de las evidencias digitales recopiladas y almacenadas de forma adecuada, pasemos a esta fase quizás más laboriosa, cuyo objetivo es reconstruir con todos los datos disponibles la línea temporal del ataque o *timeline*, determinando la cadena de acontecimientos que tuvieron lugar desde el instante inmediatamente anterior al inicio del ataque, hasta el momento de su descubrimiento.

Este análisis se dará por concluido cuando conozcamos cómo se produjo el ataque, quien o quienes lo llevaron a cabo, bajo qué circunstancias se produjo, cuál era el objetivo del ataque, qué daños causaron, etc.

La cuarta fase es la *Preparación para el análisis* en el entorno de trabajo: Previamente se deberá acondicionar un entorno de trabajo adecuado al estudio que desee realizar. Si se decanta por no tocar los discos duros originales que por cierto es muy recomendable, y trabajar con las imágenes que recopiló como evidencias, o mejor aún con una copia de estas, tenga en cuenta que necesitará montar esas imágenes tal cual estaban en el sistema comprometido.

Si dispone de recursos suficientes prepare dos estaciones de trabajo, en una de ellas, que contendrá al menos dos discos duros, instale un sistema operativo que actuará de anfitrión y que le servirá para realizar el estudio de las evidencias. En ese mismo ordenador y sobre un segundo disco duro, vuelque las imágenes manteniendo la estructura de particiones y del sistema de archivos tal y como estaban en el equipo atacado. En el otro equipo instale un sistema operativo configurado exactamente igual que el del equipo atacado, además mantenga nuevamente la misma estructura de particiones y ficheros en sus discos duros. La idea es utilizar este segundo ordenador como *conejillo de Indias* y realizar sobre las pruebas y verificaciones conforme vayan surgiendo hipótesis sobre el ataque.

La quinta fase es la *Reconstrucción de la secuencia temporal del ataque***:** El primer paso que deberá dar es crear una línea temporal de sucesos o *timeline*, para ello se recopila la siguiente información sobre los ficheros:

- Inodos asociados.
- Marcas de tiempo MACD (fecha y hora de modificación, acceso, creación y borrado).
- Ruta completa.
- Tamaño en bytes y tipo de fichero.
- Usuarios y grupos a quien pertenece.
- Permisos de acceso.
- Si fue borrado o no.

Sin duda esta será la información que más tiempo le llevará recopilar, pero será el punto de partida para su análisis.

Para comenzar ordene los archivos por sus fechas MAC, esta primera comprobación, aunque simple, es muy interesante pues la mayoría de los archivos tendrán la fecha de instalación del sistema operativo, por lo que un sistema que se instaló hace meses y que fue comprometido recientemente presentará en los ficheros nuevos, inodos y fechas MAC muy distintas a las de los ficheros más antiguos.

La idea es buscar ficheros y directorios que han sido creados, modificados o borrados recientemente, o instalaciones de programas posteriores a la del sistema operativo y que además se encuentren en rutas poco comunes. Piense que la mayoría de los atacantes y sus herramientas crearán directorios y descargarán sus *aplicaciones* en lugares donde no se suele mirar, como por ejemplo en los directorios temporales.

La sexta fase es la *Identificación del autor o autores del incidente:* Esta fase será de especial importancia si tiene pensado llevar a cabo acciones legales posteriores o investigaciones internas a su organización. Si no va a seguir estos pasos, puede saltarse esta fase y dedicar ese tiempo a otros menesteres, como por ejemplo recuperar completamente el sistema atacado y mejorar su seguridad.

Pero si decide perseguir a sus atacantes, deberá realizar algunas pesquisas como parte del proceso de identificación:

averiguar la dirección IP de su atacante, También podría encontrar esta información en fragmentos de las evidencias volátiles, la memoria virtual o archivos temporales y borrados, como restos de e- mail, conexiones fallidas, etc.

Si cree tener una IP sospechosa, compruebe en el registro RIPE NCC (www.ripe.net) a quién pertenece. Pero ojo, no saque conclusiones prematuras, muchos atacantes falsifican la dirección IP con técnicas de

spoofing. Suponga que encuentra una dirección IP y tras consultar el registro RIPE, le aparece que está asignada a una importante entidad bancaria ¿cree sinceramente que un empleado de banca le ha atacado? Otra técnica de ataque habitual consiste en utilizar *ordenadores zombis*, estos son comprometidos en primera instancia por el atacante y posteriormente son utilizados como lanzaderas del ataque final sin que sus propietarios sepan que están siendo cómplices de tal hecho. Por ello, para identificar a su atacante tendrá que verificar y validar la dirección IP obtenida.

La séptima fase es la *Evaluación del impacto causado al sistema* es el análisis forense el que le ofrece la posibilidad de investigar qué es lo que han hecho los atacantes una vez que accedieron a sus sistemas. Esto le permitirá evaluar el compromiso de sus equipos y realizar una estimación del impacto causado. Generalmente se pueden dar dos tipos de ataques:

- Ataques pasivos: en los que no se altera la información ni la operación normal de los sistemas, limitándose el atacante a fisgonear por ellos.
- Ataques activos, en los que se altera, y en ocasiones seriamente, tanto la información como la capacidad de operación del sistema.

La fase octava es la Documentación *del incidente***:** significa la importancia de tomar notas sobre todas las actividades que se lleven a cabo. Cada paso dado debe ser documentado y fechado desde que se descubre el incidente hasta que finalice el proceso de análisis forense, esto le hará ser más eficiente y efectivo al tiempo que reducirá las posibilidades de error a la hora de gestionar el incidente.

La novena fase es la *Utilización de formularios de registro del incidente***:** Alguno de los formularios que debería preparar serán:

- Documento de custodia de la evidencia.
- Formulario de identificación del equipos y componentes.
- Formulario de incidencias tipificadas.

- Formulario de publicación del incidente.
- Formulario de recogida de evidencias.
- Formulario de discos duros.

La penúltima fase es *El Informe Técnico***:** consiste en una exposición detallada del análisis efectuado. Deberá describir en profundidad la metodología, técnicas y hallazgos del equipo forense. Este deberá contener, al menos, los siguientes puntos:

- Antecedentes del incidente.
- Recolección de los datos.
- Descripción de la evidencia.
- Entorno del análisis.
- Descripción de las herramientas.
- Análisis de la evidencia.
- Información del sistema analizado.
- Características del SO.
- Aplicaciones.
- Servicios.
- Vulnerabilidades.
- Metodología.
- Descripción de los hallazgos.
- Huellas de la intrusión.
- Herramientas usadas por el atacante.
- Alcance de la intrusión.
- El origen del ataque
- Cronología de la intrusión.
- Conclusiones.
- Recomendaciones específicas.
- Referencias.

Finalmente, *El Informe Ejecutivo:* Este consiste en un resumen del análisis efectuado, pero empleando una explicación no técnica, con lenguaje común, en el que se expondrá los hechos más destacables de lo ocurrido en el sistema analizado. Constará de pocas páginas, entre tres y cinco, y será de especial interés para exponer lo sucedido al personal no especializado en sistemas informáticos, como pueda ser el departamento de Recursos Humanos, Administración, e incluso algunos directivos. En este informe deberá, donde se describir, al menos, lo siguiente:

- Motivos de la intrusión.
- Desarrollo de la intrusión
- Resultados del análisis.
- Recomendaciones.

2.7.3 **Estados Unidos Mexicanos.**

El Estado de Sinaloa – México fue pionero en llamar *Delito Informático* al delito cometido mediante un ordenador, se encuentra en el Código Penal del Estado Sinaloa en el cuerpo legal denominado Delitos Informáticos, Libro Primero Parte General Título Preliminar: De Las Garantías Penales; Capítulo Único; De Las Garantías Penales, en su Artículo 217. Comete *delito Informático*, la persona que dolosamente y sin derecho: I) Use o entre a una Base de Datos, Sistema de computadoras o a cualquier parte de la misma, con el propósito de diseñar, ejecutar o alterar un esquema o artificio, con el fin de defraudar, obtener dinero o bienes o información; o II) Intercepte, interfiera, reciba, use, altere, dañe o destruya un soporte lógico o programa de computadora o los datos contenidos en la misma, en la base, sistema o red. (Codigo Penal de Sinaloa Mx, 1992)

Los 32 Estados se rigen por el Código Penal Federal mexicano; los *Delitos Informáticos* se encuentran en el Capítulo II en el (Art.211) incisos del (1) al (7) .

Art. 211 bis**.** A quien revele, divulgue o utilice indebidamente o en perjuicio de otro, información o imágenes obtenidas en una intervención de comunicación privada, se

le aplicarán sanciones de seis a doce años de prisión y de trescientos a seiscientos días multa.
(Artículo adicionado mediante Decreto publicado en el Diario Oficial de la Federación el 7 de noviembre de 1996).

Acceso Ilícito a Sistemas y Equipos de Informática.

(Adicionado mediante Decreto publicado en el Diario Oficial de la Federación el 17 de mayo de 1999)

Art. 211 bis 1. Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad.

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad.

Art. 211 bis 2. Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad.

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad.

A quien sin autorización conozca, obtenga, copie o utilice información contenida en cualquier sistema, equipo o medio de almacenamiento informáticos de seguridad pública, protegido por algún medio de seguridad, se le impondrá pena de cuatro a diez años de prisión y multa de quinientos a mil días de salario mínimo general vigente en el Distrito Federal.

Si el responsable es o hubiera sido servidor público en una institución de seguridad pública, se impondrá, además, destitución e inhabilitación de cuatro a diez años para desempeñarse en otro empleo, puesto, cargo o comisión pública.

Art. 211 bis 4. Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática de las instituciones que

integran el sistema financiero, protegidos por algún mecanismo de seguridad, Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad.

Art. 211 bis 5. Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente modifique, destruya o provoque pérdida de información que contengan.

Art. 211 bis 6. Para los efectos de los artículos 211 Bis 4 y 211 Bis 5 anteriores, se entiende por instituciones que integran el sistema financiero, las señaladas en el artículo 400 Bis de este Código Art. 211 bis 7. Las penas previstas en este capítulo se aumentarán hasta en una mitad cuando la información obtenida se utilice en provecho propio o ajeno.

En el ordenamiento jurídico de México, lo cometido mediante un ordenador, se encuentra en el Código Penal del Estado Sinaloa en el cuerpo legal denominado Delitos Informáticos, Libro Primero Parte General Título Preliminar; De Las Garantías Penales, Capítulo Único; De Las Garantías Penales, en su Artículo 217. Comete *delito Informático*, la persona que dolosamente y sin derecho: I) Use o entre a una Base de Datos, Sistema de computadoras o a cualquier parte de la misma, con el propósito de diseñar, ejecutar o alterar un esquema o artificio, con el fin de defraudar, obtener dinero o bienes o información; o II) Intercepte, interfiera, reciba, use, altere, dañe o destruya un soporte lógico o programa de computadora o los datos contenidos en la misma, en la base, sistema o red.

Respecto a las características se dice que la Evidencia Digital, puede ser duplicada de manera exacta y copiada tal como si fuese el original, con herramientas adecuadas es relativamente fácil identificar si la evidencia ha sido alterada, comparada con la original.

Aún si es borrada, es posible, en la mayoría de los casos, recuperar la información.

Cuando los criminales o sospechosos tratan de destruir la evidencia, existen copias que permanecen en otros sitios del sistema.

El *Protocolo* de actuación para la obtención y tratamiento de los recursos informáticos y/o las evidencias digitales en la legislación mexicana se describe a continuación. (SEGOB, 2016)

Protocolo De Actuación Para La Obtención y Tratamiento De Recursos Informáticos y/o Evidencias Digitales

I. **ACTIVIDADES:** Constituirse en el o los lugares autorizados para la investigación, posteriormente verificar las condiciones mínimas de seguridad. Inspeccionar la escena de la investigación y luego desarrollar un plan para la obtención de evidencia digital. Detectar y en su caso asegurar fuentes potenciales de datos que aporten evidencia digital. Fotografiar recursos informáticos, pantallas y conexiones.

II. **RECOLECCIÓN:** El personal autorizado por la Dirección General de Tecnologías de la Información, independientemente de su adscripción. Realiza los siguientes pasos: 1. Obtener la imagen forense de la evidencia digital, conforme a los Lineamientos del Protocolo de actuación para la obtención y tratamiento de recursos informáticos y/o evidencias digitales. 2. Asegurar y preservar el recurso informático que contiene la evidencia digital original. 3. Registrar la información dinámica o en procesamiento, así como en tránsito o desplazamiento. 4. Verificar la integridad de los datos de la imagen forense.

III. **REGISTRO:** El personal autorizado por la Dirección General de Tecnologías de la Información, independientemente de su adscripción, realiza el inventario del recurso informático y/o la evidencia digital.

IV. **EMBALAJE:** El personal autorizado por la Dirección General de Tecnologías de la Información, independientemente de su adscripción. Dispone del recurso informático y/o evidencia digital para almacenarlo, sellarlo, etiquetarlo y contenerlo conforme a los Lineamientos del Protocolo de actuación para la obtención y tratamiento de recursos informáticos y/o evidencias digitales. De. La misma forma mantener cadena de custodia de la

evidencia digital, lo siguiente elaborar el Formato de la entrega-recepción de recursos informáticos y/o evidencia digital. Requisitar el Registro de Cadena de Custodia.

V. TRASLADO Y ENTREGA PARA ANÁLISIS: El personal designado por la autoridad solicitante, con apoyo del autorizado por la Dirección General de Tecnologías de la Información, independientemente de su adscripción.

VI. ANÁLISIS E INFORMES

RESPONSABLE: Personal autorizado por la Dirección General de Tecnologías de la Información, independientemente de su adscripción.

ACTIVIDADES:

Realizar el análisis correspondiente al recurso informático y/o evidencia digital.

Realizar el informe técnico que deberá contener, al menos, los siguientes puntos:

Descripción de la evidencia.

Información relevante del sistema analizado.

Análisis de la evidencia digital documentada.

Metodología utilizada.

Descripción de los hallazgos.

Conclusiones claras, firmes y congruentes.

VII. ALMACENAMIENTO EN EL LUGAR DE RESGUARDO

RESPONSABLE: Personal autorizado por el titular del órgano auxiliar o unidad administrativa.

ACTIVIDADES:

Recibir y registrar el ingreso, salidas temporales y definitivas del material embalado.

El material embalado deberá estar acompañado del Registro de Cadena de Custodia y Formato de la entrega-recepción de recursos informáticos y/o evidencia digital.

Observar y documentar las condiciones en que se recibe el material embalado en el Registro de Cadena de Custodia.

Custodiar el material embalado en el lugar de resguardo cumpliendo con las especificaciones de almacenamiento de acuerdo a su tipo, atendiendo a los Lineamientos del Protocolo de actuación para la obtención y tratamiento de evidencias digitales y/o recursos informáticos.

VIII. TRASLADO PARA LA PRESENTACIÓN DE LOS RECURSOS INFORMÁTICOS Y/O EVIDENCIA DIGITAL COMO MATERIAL PROBATORIO

RESPONSABLE: Personal autorizado por la Dirección General de Tecnologías de la Información.

ACTIVIDADES:

Requisitar el Registro de Cadena de Custodia y el Formato de la entrega-recepción de recursos informáticos y/o evidencia digital.

IX. DESTINO FINAL

RESPONSABLE: Titular del órgano auxiliar o unidad administrativa.

ACTIVIDAD:

El área competente determinará el destino final de los recursos informáticos. Dicha determinación se incluirá en el Registro de Cadena de Custodia.

El protocolo para la obtención de la evidencia digital de México se encuentra al mismo nivel que los protocolos de los Estados Unidos y España pese a no haberse adherido a la Convenio de Budapest. Además, que describe que dentro del personal autorizado para el proceso de recolección, análisis e interpretación de la evidencia

digital es de ingenieros de sistemas e ingenieros en telecomunicaciones. El ingeniero en telecomunicaciones tiene en su poder manejar la información. Los datos pasan a través de sus manos. La información es poder y tener la capacidad de conocerla y trasmitirla es mucha responsabilidad, pero a su vez es también es una garantía.

2.7.4 **República de Argentina**

A partir de 2008, la Ley 26.388 conocida como la *ley de Delitos Informáticos* ha incorporado y realizado una serie de modificaciones al Código Penal de Argentina en los artículos 77, 128, El Epígrafe del Capítulo III del Título V del Libro 2, 153 153 Bis, 155,157, 157Bis, 183, inciso 16 del 173, 183, 184, 197, 255. (Senado Argentino, 2008)

Se modificó el Epígrafe al capítulo III cuyo nuevo título es: *Violación de Secretos y de la Privacidad*. Los artículos que modifica o agrega son el 128 Pornografía infantil -153 Interceptación ilícita y 153 Bis Acceso ilícito, 155 y 157 y 157 Bis, fue incorporado por la ley 25.326 de Protección de Datos Personales (2000) y fue modificado por la ley 25.326, 173, 183 en su 2do parágrafo Atentado contra la integridad de los datos, 184, 197 Atentando con la integridad del sistema , 255. El 292 Falsedad informática, 173 Fraude o estafa informática. (Temperi, 2013)

En el año 2013 se promulgó la Ley 26.904, que plantea que el grooming, en Argentina, es un delito. El artículo 1 de la misma expresa que se incorpora al Código Penal el artículo 131, el cual dice que: *será penado con prisión de seis (6) meses a cuatro (4) años el que, por medio de comunicaciones electrónicas, telecomunicaciones o cualquier otra tecnología de transmisión de datos, contactare a una persona menor de edad, con el propósito de cometer cualquier delito contra la integridad sexual de la misma*. (Codigo Penal de la Nacion Argentina, 2019)

Hasta el 2018 no existía una reforma en materia procesal penal respecto a los delitos informáticos, debido a que la ley 26388 tuvo en consideración los lineamientos de la Convención sobre Ciberdelincuencia de Budapest del 23 de noviembre de 2001 pero solo parcialmente. Es decir, la legislación argentina se adaptó únicamente al derecho

penal sustantivo descrito en el Capítulo II Sección I de la mencionada Convención y no así del Sección II que se refiere al derecho procesal penal. Por lo tanto, no se adoptaron medidas para la obtención de la *Evidencia Digital* de cualquier delito cometido por medio de un sistema informático. (Borzi, 2018)

Es por esta razón que la legislación en el derecho procesal penal respecto a estos delitos se limita a:

- Ciber patrullaje mediante la geolocalización mediante un GPS
- Interceptación en telecomunicación en móviles previa orden judicial fundada.
- Acceso a cuentas de correo y mensajería de móviles inteligentes, pero esto dificulta la investigación de agencias policiales y judiciales ya que la información se encuentra encriptada.
- Acceso a Bases de Datos de las agencias públicas como es: La Administración Federal de Ingresos Públicos, Administración de la Seguridad Social, Dirección Nacional de Migración, Dirección Nacional de Aduana y Banco de la República de Argentina que suelen aportar con elementos para la continuidad de una pesquisa. (Borzi, 2018)

En 2020 la interventora de la Agencia Federal de Inteligencia, Cristina Caamaño, aprobó el Protocolo para la Estandarización del Procedimiento de Obtención de Evidencia Digital, que regula el procedimiento de obtención y manejo de este tipo de material a fin de garantizar su validez, tanto para su incorporación en investigaciones internas, como para la eventual formulación de una denuncia penal. (Ciberdelito, 2022)

Según la Agencia Federal de Inteligencia de Argentina (AFI); este protocolo regula el procedimiento de obtención y manejo de este tipo de material a fin de garantizar su validez, tanto para su incorporación en investigaciones internas, como para la eventual formulación de una denuncia penal.

Este nuevo instrumento, que deberá aplicarse en todos los procedimientos investigativos llevados adelante por las áreas de la Agencia, establece lineamientos generales para la obtención y preservación de elementos digitales de potencial relevancia para una investigación administrativa y, eventualmente, judicial.

El protocolo contempla el tratamiento del soporte físico que contenga el material, como pueden ser discos rígidos, pendrives, teléfonos o cualquier dispositivo de almacenamiento, así como de la información digital propiamente.

Por tanto, el protocolo formaliza el proceso de obtención de la imagen forense del contenido digital y la asignación de su código hash, una secuencia numérica no reversible que permite corroborar la identidad de un archivo y preservar la integridad de los datos.

La elaboración de procedimientos estandarizados aplicables a la labor de las distintas áreas de la Agencia Federal de Inteligencia constituye uno de los objetivos de la intervención, con el objetivo de mejorar los mecanismos de control. (AFI, 2020)

La resolución 528/21 del Ministerio de Seguridad de la República de Argentina en la que se aprueba el **Protocolo De Actuación Para La Investigación Científica En El Lugar Del Hecho** del 25 de noviembre de 2021 y publicada en el Boletín Nacional del 26 de noviembre de 2021. La descripción del *Protocolo* en sus partes más importantes son : (CONICET, 2021)

- El especialista en informática forense será el responsable del secuestro de la exploración, localización, valoración, extracción y/o *secuestro de Potenciales Elementos de Prueba digitales* que se encuentren asociados al hecho investigado y que sea de interés para el análisis pericial en el laboratorio de su especialidad, procurando la relevancia, suficiencia, validez legal y confiabilidad durante el proceso de *identificación, recolección y adquisición* de los mismos.

Estos conceptos se encuentran determinados por la Guía Integral de Empleo de la Informática Forense en el Proceso Penal y el documento *Guidelines to Digital Forensics First Responders* de Interpol, recomendada como bibliografía de consulta en el presente protocolo.

1. El especialista en informática forense deberá intervenir de acuerdo con los protocolos específicos y actualizados en la materia y aplicando las buenas prácticas reconocidas de su especialidad.
2. Cuando los Potenciales Elementos de Prueba (PEP) digitales sean muy voluminosos o exista excesiva cantidad de ellos en el lugar del hecho y se tenga conocimiento preciso de los datos o clase de datos que se buscan, o se encuentren afectados derechos de terceros, se recomienda el uso de herramientas de muestreo rápido *triage* para precisar el grado de relevancia de cada dispositivo electrónico, previa consulta y autorización con la autoridad judicial interviniente.
3. Resulta aconsejable que la intervención del especialista en informática forense sea posterior a la exploración y levantamiento de Potenciales Elementos de Prueba (PEP) de interés *papiloscópico* y/o químico biológico que pudieran encontrarse sobre los medios tecnológicos informáticos. En tal caso, los especialistas en papiloscopía y químico biológico deberán consultar y acordar con el especialista en informática forense el procedimiento y la aplicación de reactivos que resulten menos dañinos para el dispositivo explorado. Asimismo, en caso de que el especialista en informática forense deba intervenir antes que los otros especialistas, deberá hacerlo con el empleo de guantes y la protección adecuada que impida o disminuya lo más posible la alteración o destrucción de Potenciales Elementos de Prueba que pudieran encontrarse sobre los dispositivos.
4. La extracción de datos en *vivo* de los dispositivos podrá realizarse siempre con consulta y autorización previa de la autoridad judicial interviniente.

5. La extracción de datos en la *nube* podrá realizarse siempre con consulta y autorización previa de la autoridad judicial interviniente, quien determinará el objeto y alcance de dicha medida.
6. Ante la presencia de *criptoactivos* se deberá realizar consulta con la autoridad judicial o fiscal interviniente, quien determinará el temperamento a adoptar.
7. El especialista en informática forense procurará que en el acta y/o en el informe de su especialidad conste una fijación narrativa, precisa y detallada que suministre una noción clara del lugar donde fueron hallados los medios tecnológicos informáticos, de toda incidencia que hubiere acontecido durante el procedimiento policial, de los *Potenciales Elementos de Prueba* (PEP) de su interés detectados en el lugar del hecho y el estado en que estos fueron hallados *encendido/apagado*, incluyendo las características identificativas de cada dispositivo *por ejemplo, daños, marca, modelo, número de serie y cualquier marca de identificación*. Cuando sea necesario y las circunstancias del hecho lo ameriten, el especialista en informática forense procurará que la fijación narrativa se complemente con fotografías, filmaciones y planos del lugar y del sitio de ubicación de cada efecto. Todo ello a fin de asegurar que el procedimiento pueda ser reconstruido, en caso de ser solicitado por la autoridad judicial. (Conicet, 2021, pp. 28-30)

2.7.5 **Estado Plurinacional de Bolivia**

La legislación boliviana a partir de la promulgación de su Constitución Política del Estado Plurinacional de Bolivia del 7 de febrero de 2009, que garantiza: El Acceso a la Información, a la Ciencia, Tecnología e Investigación y Protege mediante la Acción de Protección de Privacidad y la Protección de Telecomunicaciones entre otros.

El bloque de constitucionalidad se encuentra establecido en el artículo 410 de la Constitución del Estado Plurinacional y establece que:

La Constitución es la norma del ordenamiento jurídico boliviano y goza de primacía frente a cualquier otra disposición normativa. El bloque de constitucionalidad está integrado por los Tratados y Convenios internacionales en materia de Derechos Humanos y las normas de Derecho Comunitario, ratificados por el país. La aplicación de. Las normas jurídicas se regirán por la siguiente jerarquía, de acuerdo a las competencias de las entidades territoriales:

1. Constitución Política del Estado
2. Los Tratados internacionales
3. Las leyes nacionales, los estatutos autonómicos, las cartas orgánicas y el resto de legislación departamental, municipal e indígena.
4. Los decretos, reglamentos y demás resoluciones emanadas de. Los órganos ejecutivos correspondientes.

En consecuencia, la Constitución Política del Estado es la Ley Suprema del Ordenamiento Jurídico Nacional y ninguna disposición de menor rango puede ser contraria a la misma.

La Constitución Política del Estado garantiza el derecho a la privacidad e intimidad personal y familiar. Es el Articulo 130 el recurso de Acción de Protección de Privacidad, es de ultima ratio y puede ser interpuesta cuando una persona sienta que estos datos están siendo indebidamente utilizados.

El gran avance de las TIC ha rebasado los límites del Derecho Positivo, es decir, actualmente no existen normas legales que regulen de manera específica las actividades tecnológicas; es por ello, que la sabiduría de la Constitución Política del Estado ha incorporado el capítulo de Ciencia, Tecnología e Investigación, otorgando a las Universidades el desarrollo de los procesos de investigación científica.

En relación a los derechos civiles se puede citar los incisos (2) (6) del Artículo 21 de la Constitución Política del Estado.

(2) A la privacidad, intimidad, honra, honor, propia imagen y dignidad.

(6) A acceder a la información, interpretarla, analizarla y comunicarla libremente, de manera individual o colectiva.

Otro importante instituto constitucional, tiene que ver con los derechos y garantías de las personas, entre ellos, el derecho a la privacidad e intimidad y acceso a la información.

Es cuanto el derecho a la privacidad e intimidad, es una garantía constitucional que no puede ser violentada y menos vulnerada porqué así lo ha dispuesto la Constitución Política del Estado; sin embargo, surge cuestionar el alcance y límite de estas garantías constitucionales en materia de TIC.

Actualmente, existen millones de recursos Informáticos en el Internet destinados a capturar y recolectar los datos de las personas naturales y jurídicas para lograr potencializar los bancos de datos de las personas, utilizando medios o herramientas insospechadas e inimaginables para este fin, a modo de ejemplo, cuando una persona se acerca a una entidad financiera y proporciona su número de cédula de identidad, la entidad financiera edita información de la persona hasta el más mínimo detalle o peor aun cuando en las redes sociales se editan datos personalísimos, en muchos casos contenido sexual.

Es en la Ley 1768 de 1997; Código Penal, que se modificó e insertó el Capitulo XI denominado *Delitos Informáticos*, y son dos los delitos que se describen a continuación:

Artículo 363 bis.- (Manipulación Informática).- El que con la intención de obtener un beneficio indebido para sí o un tercero, manipule un procesamiento o transferencia de datos informáticos que conduzca a un resultado incorrecto o evite un proceso tal cuyo resultado habría sido correcto, ocasionando de esta manera una transferencia patrimonial en perjuicio de tercero, será sancionado con reclusión de uno a cinco años y con multa de sesenta a doscientos días.

En el caso de la manipulación del dato o proceso o información, es que el resultado puede originar que el mismo sea incorrecto.

Artículo 363 ter.- (Alteración, Acceso y Uso Indebido De Datos Informáticos).- El que sin estar autorizado se apodere, acceda, utilice, modifique, suprima o inutilice, datos almacenados en una computadora o en cualquier soporte informático, ocasionando perjuicio al titular de la información, será sancionado con prestación de trabajo hasta un año o multa hasta doscientos días.

Este tipo penal, tiene que ver esencialmente con el acceso indebido a los dominios de las Tecnologías de la Información y Comunicación, es decir, que alguna persona acceda a los dominios informáticos sin estar autenticado o no tenga permiso de ingreso mediante *login y password.*

Derecho Procesal Penal.

En materia procesal penal, la *Evidencia Digital,* es a quien se debe estudiar y para ello se revisó los artículos relacionados con la *prueba* del Código de Procedimiento Penal.

La Prueba

La prueba, es todo motivo o razón aportado al proceso por los medios y procedimientos aceptados en la ley para llevar ante la autoridad judicial al convencimiento de la certeza sobre los hechos discutidos en un proceso. Muchos autores le asignan a la prueba el fin de establecer la verdad de los hechos y no solamente el convencimiento al juez. **(Devis Echandía H. , 2005)**

Definir la naturaleza y la función de la prueba dentro del proceso. Es, no obstante, oportuno distinguir dos aspectos de este problema, que van analizados separadamente: el primero tiene que ver con la prueba comprendida como *fuente de información,* o sea como *medio de prueba*. Medio de prueba, y a la prueba como *resultado.*

Para Taruffo, Michele; Vazquez, Ma.delCarmen; Ferrer Jordi:

> La prueba entendida como medio de prueba puede ser constituida por cualquier persona, cosa, hechos, grabaciones, reproducciones, documento, los cuales proporcionen informaciones útiles para establecer la verdad o la falsedad de un enunciado factual. Inmediatamente, surge, por lo tanto, la noción de *utilidad* que debe caracterizar el medio de prueba: se trata de una prueba en el mero sentido de la palabra, si la misma es relevante, o sea si proporciona informaciones que sirven para garantizar el hecho del cual se trata. Si falta este requisito, es decir, si las informaciones que arroja no son útiles para este propósito, no se puede ni siquiera hablar en sentido propio de medio de *prueba*
>
> En el fondo de esta noción tan general, se encuentran frecuentemente muchas distinciones que no vale la pena considerar en detalle, pero una de éstas, muy difundida en la doctrina procesal, merece algún comentario. Se trata de la distinción entre la prueba directa y la prueba indirecta. Se define como "directa" la prueba que tiene como objeto inmediato el hecho principal que se trata de probar, como en el caso de un testimonio que se realiza sobre ese hecho o un documento que lo representa, mientras que, se considera como "indirecta" la fuente de información que se refiere a otro hecho y requiere que se formule una inferencia del mismo que se considera "secundario" al hecho principal, como en el caso del indicio o de la presunción simple. Se trata de una distinción banal, que, pero puede inducir en error si se considera – como mayormente sucede– que la prueba directa no requiera ninguna operación lógica y que no solo la prueba indirecta se funda en su inferencia. En realidad, contrariamente, incluso la prueba directa requiere de un razonamiento de deducción: suficiente será considerar que son necesarias diferentes deducciones para establecer la credibilidad de un testigo o la autenticidad de un documento (Taruffo, Michele; Vazquez, Ma.delCarmen; Ferrer Jordi, 2018, p. 26)**.**

Para la persecución penal la legislación boliviana presenta el *Código de Procedimiento Penal* y es en su Artículo 13 que se encuentra la *Legalidad de la Prueba*:

Los elementos de prueba sólo tendrán valor si han sido obtenidos por medios lícitos e incorporados al proceso conforme a las disposiciones de la Constitución Política del Estado y de este Código.

No tendrá valor la prueba obtenida mediante torturas, malos tratos, coacciones, amenazas, engaños o violación de los derechos fundamentales de las personas, ni la obtenida en virtud de información originada en un procedimiento o medio ilícito.

Artículo 13º.- (Legalidad de la prueba).- Los elementos de prueba sólo tendrán valor si han sido obtenidos por medios lícitos e incorporados al proceso conforme a las disposiciones de la Constitución Política del Estado y de este Código.
No tendrá valor la prueba obtenida mediante torturas, malos tratos, coacciones, amenazas, engaños o violación de los derechos fundamentales de las personas, ni la obtenida en virtud de información originada en un procedimiento o medio ilícito.

A partir de la Constitución Política del Estado y Código de Procedimiento Penal es que el principio de la legalidad de la prueba se constituye en un derecho y garantía de las personas para la *Cadena De Custodia* de la misma. En el caso de las TIC es la *Evidencia Digital* un elemento muy susceptible de ser contaminado, especialmente, cuando concurren agentes externos. Por tanto, si la misma ha sido contaminada, no garantizará la averiguación de la verdad.

La *Evidencia Digital*, en instancias judiciales, es muy débil en su instancia de valoración, lamentablemente las autoridades del sistema judicial boliviano no han tenido capacitación suficiente en el marco de las Tecnologías de la Información vinculada al Derecho o propiamente en el Derecho Informático para una adecuada valoración de la Evidencia Digital, Edmond Locard decía que la evidencia estaba ahí y lo único que el investigador tenía que hacer era interpretarla. (Morrish, 1955)

El concepto de *Evidencia Digital,* en instancias judiciales es inexistente y la *Valoración de la Prueba* se encuentra tipificada en el Código de Procedimiento Penal en el libro de medios de prueba en el artículo siguiente:

Artículo 173º.- (Valoración). El juez o tribunal asignará el valor correspondiente a cada uno de los elementos de prueba, con aplicación de las reglas de la sana critica, justificando y otorga determinado valor, en base a la apreciación conjunta y armónica de toda prueba esencial producida.

En las Tecnologías de la Información y Comunicación vinculada al Derecho o propiamente al *Derecho Informático,* el *Principio De Intercambio* será el elegido para su valoración. Este principio es conocido también como: *El Principio de Edmond Locard,* establece que siempre que dos elementos entren en contacto entre sí, se producirá un intercambio de material. Durante un acto criminal, el perpetrador trae algo a la escena y quita algo a la escena. En otras palabras, la evidencia estaba ahí y lo único que el investigador tenía que hacer era interpretarla. (Morrish, 1955)

Sobre la *Valoración de la prueba* existe un aspecto muy importante, se refiere en cierto sentido a la naturaleza de esta *valoración*. Comenzando de una ley francesa de 1791, que, de hecho, se ha ido difundiendo en la doctrina procesal en relación al proceso penal, y no solamente una concepción según la cual la valoración de la prueba, y por lo tanto la decisión final de los hechos, debería basarse exclusivamente en la plena convicción del juez o del jurado. Se trataría entonces de una especie de autoanálisis psicológico y moral, o sea de una introspección realizada por el sujeto que debe decidir con el fin de alcanzar la *certeza*, tal vez *absoluta*, en torno a la verdad de los hechos. Sin discutir si esta concepción sea confiable, de la que es normal llegar a dudar, es necesario, de todas maneras, observar que la misma establece la valoración de las pruebas como un acto absolutamente subjetivo y esencialmente arbitrario, ya que de esa convicción plena no se puede conocer –ni controlar– nada, colocándose la misma, precisamente, en el fuero interno del sujeto que decide. Al respecto, se puede observar que la idea de una valoración irracional de las pruebas es hasta hoy bastante

difundida, y no solo en la cultura penalista francesa. Hasta cierto punto, de hecho, la misma puede reconectarse a la concepción *holística* y también a la concepción *persuasiva* de la prueba, en la praxis de diferentes tribunales en diferentes ordenamientos; es esta ultima la concepción utilizada en el ordenamiento boliviano (Teoria de la Prueba, 2018, p. 31)

La valoración analítica y racional de las pruebas requiere la formulación de un razonamiento que se desarrolle de modo estructurado y con criterios verificables: se trata en realidad de un conjunto complejo de deducciones con las cuales se conectan lógicamente entre sí sus diferentes propuestas, hasta formular un razonamiento con el cual el juez organiza las informaciones que posee, controla la fiabilidad y deriva en conclusiones en torno a la verdad o falsedad de los enunciados factuales que son objeto de su decisión. La lógica proporcional provee también al juez los instrumentos y los modelos de deducción que pueden y deben ser utilizados en cualquier decisión que pretende ser racionalmente justificada (Taruffo, Michele; Vazquez, Ma.delCarmen; Ferrer Jordi, 2018).

En materia procesal penal existe un peligro y este se encuentra descrito en el Código de Procedimiento Penal boliviano como es el *Peligro de Obstaculización* tipificado en el artículo siguiente:

Artículo 235º.- (Peligro de Obstaculización).- Por peligro de obstaculización se entiende a toda circunstancia que permita sostener de manera fundamentada, que el imputado con su comportamiento entorpecerá la averiguación de la verdad. Para decidir acerca de su concurrencia se realizará una evaluación integral de las circunstancias existentes, teniendo especialmente en cuenta las siguientes:

1. Que el imputado destruya, modifique, oculte, suprima, y/o falsifique, elementos de prueba;
2. Que el imputado influya negativamente sobre los partícipes, testigos o peritos, a objeto de que informen falsamente o se comporten de manera reticente;

3. Que el imputado influya ilegal o ilegítimamente en magistrados del Tribunal Supremo, magistrados del Tribunal Constitucional Plurinacional, vocales, jueces técnicos, jueces ciudadanos, fiscales y/o en los funcionarios y empleados del sistema de administración de justicia;
4. Que el imputado induzca a otros a realizar las acciones descritas en los numerales 1, 2 y 3 del presente Artículo;
5. Cualquier otra circunstancia debidamente acreditada que permita sostener fundadamente que el imputado, directa o indirectamente, obstaculizará la averiguación de la verdad.

En materia de las TIC, la *Evidencia Digital* es un elemento físico o lógico muy susceptible de ser contaminado, especialmente, cuando el investigado tiene la posibilidad de destruir, modificar, ocular, suprimir y/o falsificar la *Evidencia Digital* en fracciones de segundos, que van desde desenchufar el dispositivo electrónico hasta formatear el dispositivo electrónico y es en esa instancia en que se puede perder el impacto de la investigación.

En consecuencia, es recomendable realizar el proceso de investigación en forma silenciosa, es decir, que el investigado no conozca sobre el proceso de investigación para evitar la contaminación de la *Evidencia Digital*.

Es el *Anticipo de prueba* establecido en el Artículo 307 del Código de Procedimiento Penal de Bolivia que establece que en una persecución penal y cuando sea necesario practicar un reconocimiento, registro, reconstrucción o pericia, que por su naturaleza o características se consideren como actos definitivos e irreproducibles, o cuando deba recibirse una declaración que, por algún obstáculo, se presuma que no podrá producirse durante el juicio, el fiscal o cualquiera de las partes podrán pedir al juez que realice estos actos.

Artículo 307º.- (Anticipo de prueba).- Cuando sea necesario practicar un reconocimiento, registro, reconstrucción o pericia, que por su naturaleza o características se consideren como actos definitivos e irreproducibles, o cuando deba recibirse una declaración que, por algún obstáculo, se presuma que no podrá producirse durante el juicio, el fiscal o cualquiera de las partes podrán pedir al juez que realice estos actos.

El juez practicará el acto, si lo considera admisible, citando a todas las partes, las que tendrán derecho a participar con las facultades y obligaciones previstas en este Código.

Si el juez rechaza el pedido, se podrá acudir directamente al tribunal de apelación, quien deberá resolver dentro de las veinticuatro horas de recibida la solicitud, ordenando la realización del acto, si lo considera admisible, sin recurso ulterior.

A partir de la Constitución Política del Estado y Código de Procedimiento Penal, el principio de la legalidad de la prueba se constituye en un derecho y garantía de las personas para la cadena de custodia de la misma. En el caso de las TIC, la *Evidencia Digital* se constituye como un elemento muy susceptible de ser contaminado, especialmente, cuando concurren agentes externos que no garantizan la averiguación de la verdad.

Respecto a los riesgos procesales del imputado el *Código de Procedimiento Penal* dispone en su artículo 235 *Peligro de Obstaculización* que, se entiende a toda circunstancia que permita sostener de manera fundamentada, que el imputado con su comportamiento entorpecerá la averiguación de la verdad. Para decidir acerca de su concurrencia se realizará una evaluación integral de las circunstancias existentes, teniendo especialmente en cuenta el inciso (1) al (5) cuando de delitos informáticos se investigue.

Estos incisos establecen lo siguiente:

1) Que el imputado destruya, modifique, oculte, suprima, y/o falsifique, elementos de prueba;

2) Que el imputado influya negativamente sobre los partícipes, testigos o peritos, a objeto de que informen falsamente o se comporten de manera reticente;

3) Que el imputado influya ilegal o ilegítimamente en magistrados del Tribunal Supremo, magistrados del Tribunal Constitucional Plurinacional, vocales, jueces técnicos, jueces ciudadanos, fiscales y/o en los funcionarios y empleados del sistema de administración de justicia;

4) Que el imputado induzca a otros a realizar las acciones descritas en los numerales 1, 2 y 3 del presente Artículo;

5) Cualquier otra circunstancia debidamente acreditada que permita sostener fundadamente que el imputado, directa o indirectamente, obstaculizará la averiguación de la verdad.

Cadena de Custodia.

El Código de Procedimiento Penal describe en el Articulo 74 la actuación de la *Policía Boliviana Nacional* en la investigación de los delitos, se encargará de la identificación y aprehensión de los presuntos responsables, de la identificación y auxilio a las víctimas, de la *acumulación y seguridad de las pruebas* y de toda actuación dispuesta por el fiscal que dirige la investigación; diligencias que serán remitidas a los órganos competentes.

El Artículo 75 del mismo Código, describe que el Instituto de Investigaciones Forenses (IDIF) es un órgano dependiente administrativa, y financieramente de la Fiscalía General de la República. Estará encargado de realizar, con autonomía funcional, todos los *estudios científico - técnicos* requeridos para *la investigación* de los delitos o la *comprobación* de otros hechos mediante orden judicial.

Las facultades de la Policía Nacional se encuentra en descritas en el Artículo 29 del Código de Procedimiento Penal; Los miembros de la Policía Nacional, cuando cumplan funciones de policía judicial, en el marco de las disposiciones establecidas

en el Código de Procedimiento Penal específicamente en los incisos (10); *Recoger y conservar los objetos e instrumentos relacionados con el delito*; (11); Secuestrar, con autorización del fiscal, documentos, libros contables, fotografías y *todo elemento material que pueda servir a la investigación*; y (12); *Custodiar, bajo inventario*, los objetos secuestrados.

La Ley 260 de 11 de Julio de 2012, es la Ley Orgánica del Ministerio Publico Art. 40 y es el inciso (10) de las atribuciones de los Fiscales de Materia y estos deben asegurarse que todos los *indicios y elementos de prueba* recolectados sean debidamente resguardados dentro de la *cadena de custodia,* en particular los recolectados de la víctima. (Ministerio Publico, 2012)

La Policía Nacional, el Ministerio Publico y los peritos tienen un Manual de Actuaciones Investigativas de Fiscales, Policías y Peritos.- El manual es la secuencia y sucesión lógica de las etapas del proceso penal, que enuncia y explica las actuaciones que podrían realizar fiscales y policías, en la investigación de un delito cualquiera. (Manual de Actuaciones Investigativas de Fiscales, Policías y Peritos, 2007)

Del análisis de la normativa penal nacional se puede afirmar que no existe normativa específica con relación a la manera en la que debe procederse ante la presencia de la evidencia digital hecho que perjudica la averiguación de la verdad en todos aquellos ilícitos relacionados con las TIC. En los países analizados en el presente estudio se evidencia que se tienen por lo menos protocolos o normas internacionales que se utilizan como referencia para la recolección de la evidencia digital. En Bolivia, estos protocolos no son tomados en cuenta por las autoridades técnicas llamadas a levantar la evidencia digital cuando ésta se presenta.

Legislación boliviana en Derecho Informático.

Se tiene a la legislación informática como un conjunto de reglas jurídicas de carácter preventivo y correctivo, derivadas del uso y explotación de la informática, entre ellas:

La Constitución Política del Estado, garantiza y protege los derechos siguientes : i) Acceso a la Información, ii) Ciencia, Tecnología e Investigación, iii) Acción de Privacidad, iv) Telecomunicaciones; El Código Penal a los Delitos Informáticos; El Código Civil a los Contratos con denominaciones especiales; La Ley del Derecho de Autor; La Ley Integral de lucha contra la Trata y Tráfico de Personas y la Ley General de Telecomunicaciones, Tecnologías de la Información y la Comunicación.

Legislación boliviana conexa con las Tecnologías de la Información:

Ley de Derecho de autor (Ley 1322) de 13 de abril de 1992. En el Articulo 6 incluye la protección del derecho de autor de los programas de ordenador o computación(*soporte lógico o software* bajo reglamentación específica;

Ley de Organización Judicial (Ley 3324) del 18 de enero de 2006; Articulo 14. Incorpórese en el Capítulo VI Distribución de Procesos, del Título V Corte Superior de Distrito, el Artículo 123 bis con el siguiente texto:

Artículo 123 bis. (Buzón Judicial). En la Corte Suprema de Justicia, Cortes Superiores de Distrito y Juzgados en provincias, funcionará el servicio del buzón judicial, donde se centralizará la presentación de memoriales fuera del horario judicial y en días inhábiles, en caso de urgencia y cuando esté por vencer un plazo perentorio. Este servicio utilizará medios electrónicos que aseguren la presentación en términos de día, fecha y hora.

Alternativamente se aplicará lo previsto en el Art. 97 del Código de Procedimiento Civil".

Código Penal (Ley 1768) de 13 de Marzo de 1997, modificaciones al Código Penal, se incluye el Capítulo XI Delitos *Informáticos*, Art. 363 bis Manipulación Informática y 363 ter Alteración, Acceso y Uso Indebido de Datos Informáticos;

Decreto Supremo 24582 de 25 de abril de 1997. Reglamento de Soporte Lógico, que vela por la protección de los derechos de autor en software;

Decreto Supremo 24967 de 02 de febrero de 1998. Creación del Consejo de Ciencia y Tecnología. Cambia la dependencia de BOLNET a la Vicepresidencia;

Ley 1836 de 01 de abril de 1998 del Tribunal Constitucional, Art 29 Admite demandas y recursos por FAX;

Decreto Supremo 26134 de 30 de marzo de 2001, crea una comisión interinstitucional para elaborar una estrategia de negociación sobre regulación de licencias de software en el Poder Ejecutivo;

Ley de Fomento a la Ciencia, Tecnología e Innovación (Ley 2209) de 08 de Junio de 2001;

Decreto Supremo 26455 de 19 de diciembre de 2001 SIGMA, la administración pública habilita un sistema informático para sus procesos administrativos;

Decreto Supremo 26553 de 19 de marzo de 2002, creación de ADSIB para la implementación de nuevas tecnologías de la información;

Decreto Supremo 26624 de 14 de mayo de 2002, reglamento para ordenar el registro de nombres de dominio en Bolivia para Internet;

Ley 2492 de 02 de Agosto de 2003. Código Tributario, Art. 77, admite como medios de prueba los contenidos en medios informáticos. Art 79 incorpora medios tecnológicos para procesos tributarios y aprueba las notificaciones electrónicas;

Decreto Supremo 27241 de 14 de noviembre de 2003, reglamento de procedimientos administrativos, admite como medios de prueba los documentos electrónicos;

Decreto Supremo 27310 de 09 de enero de 2004, reglamento del Código Tributario, reconoce medios e instrumentos tecnológicos y permite notificaciones por medios electrónicos;

Ley 2631 de 20 de febrero de 2004, reforma a la Constitución Política del Estado. Art 23 incluye el habeas data como recurso constitucional extraordinario, que garantiza la privacidad e intimidad personal mediante la protección de datos personales;

Resolución 086/2004 de 22 de Septiembre de 2004, reglamenta la firma digital;

Ley 3324 de 18 de enero de 2006 Ley de reformas orgánicas y procesales a la Ley de Organización Judicial;

Ley 164 de 08 de Agosto de 2011, Ley General de Telecomunicaciones, Tecnologías de la Información y Comunicación.

En materia de TIC, la *Evidencia Digital* es un elemento físico o lógico muy susceptible de ser contaminado, especialmente, cuando el investigado tiene la posibilidad de destruir, modificar, ocultar, suprimir y/o falsificar la evidencia digital en fracciones de segundos, que van desde desenchufar el dispositivo electrónico hasta formatear el dispositivo electrónico y es en esa instancia en que se puede perder el impacto de la investigación.

En consecuencia, es recomendable realizar el proceso de investigación en forma silenciosa, es decir, que el investigado no conozca sobre el proceso de investigación para evitar la contaminación de la *Evidencia Digital*.

Otros Tipos Penales.

Dentro de la legislación penal boliviana, existen también otros tipos que se encuadran a los delitos en Tecnologías de la Información, en sentido, que el actuar delincuencial puede ser producido *por cualquier medio*, a modo de ejemplo: Art. 281 quater Difusión e Incitación al Racismo o a la Discriminación; Art. 281 octies Insultos y otras Agresiones Verbales por motivos racistas; Art. 283 Calumnia; Art. 285 Propalación de Ofensas; Art. 287 Injuria; Art. 300 Violación de la Correspondencia y Papeles Privados; Art. 312 quater Acoso Sexual; Art. 318 Corrupción de Menores; Art. 320 Corrupción de Mayores; Art. 323 bis Pornografía de Niñas, Niños o Adolescentes y de Personas Incapaces; Art. 333. Extorción; Art. 339 Destrucción de cosas propias para defraudar y Ley 3325 Trata y Tráfico de personas y otros delitos relacionados.

En la actual economía jurídica nacional, así como en el Derecho comparado, no existen bases legales sobre el reconocimiento pleno y válido para el *Uso Algorítmico en el Proceso de Búsqueda de la Evidencia Digital en Delitos Informáticos*; las

acciones antijurídicas producidas al entorno o dentro de las TIC; en consecuencia, denotan una flagrante inseguridad jurídica sobre el problema expuesto en la presente investigación.

Luego de haber realizado un estudio a nuestra legislación en Tecnologías de la Información Comunicación, se puede concluir que la misma es muy limitada, especialmente en el campo reglamentario y procedimental en cuanto al **USO ALGORITMICO EN EL PROCESO DE BUSQUEDA DE LA EVIDENCIA DIGITAL EN DELITOS INFORMATICOS.**

Con el objetivo de presentar la información obtenida de manera sistemática se ha desarrollado la siguiente tabla:

PAIS	**CUERPO LEGAL**	**DELITOS INFORMATICOS**	**PROTOCOLO PARA LA OBTENCION DE LA EVIDENCIA DIGITAL**
EEUU	**Actas**. (Statutes) Common Law; Case law. Cibercrime.	**Fraude y acceso ilegal:** ▪ Usurpación de identidad y Fraude ▪ Terrorismo **Obscenidades** ▪ Pornografía infantil ▪ Prohibición de dominios engañosos. ▪ Prohibición de uso de recursos públicos para adquisición de	**FBI** ▪ Levantamiento: Realizar una copia exacta de los medios informáticos a ser analizados, sin alterar la escena de investigación. ▪ Proceso de recuperación de datos y el Hash. ▪ Cadena de custodia de la evidencia digital.

PAIS	CUERPO LEGAL	DELITOS INFORMATICOS	PROTOCOLO PARA LA OBTENCION DE LA EVIDENCIA DIGITAL
		ordenadores sin filtros. ▪ Seducción de menores para propósitos sexuales. **Copyright** **Difamación** **Amenazas y** **Acoso cibernético**	▪ Hash servirá para la validación de hallazgos y verificación de la no alteración en el análisis forense. ▪ Documentar el aseguramiento de la evidencia digital. ▪ Preservación de la evidencia digital ▪ Almacenamiento de la evidencia digital en medios electrónicos ▪ Elaboración de informes de investigación, actuación y análisis. **Guía Hong Kong** ▪ Recolección de Evidencia. ▪ Consideraciones legales Reportes en la Corte. **Digital Forensic Process**. fases: ▪ Fase de Adquisición de la evidencia digital

PAIS	CUERPO LEGAL	DELITOS INFORMATICOS	PROTOCOLO PARA LA OBTENCION DE LA EVIDENCIA DIGITAL
			▪ Fase de Autenticación de la evidencia digital ▪ Fase de Análisis de la evidencia digital. ▪ Fase para estandarizar formatos de los datos forenses ▪ Aplicación de metodologías interoperabilidad con otros organismos. **IDIP** ▪ Preparación ▪ Despliegue ▪ Investigación de la escena física ▪ Investigación de la escena digital ▪ Presentación de conclusiones **Normas Internacionales** **RFC3227** Para la recuperación de la evidencia digital. **ISO/IEC 27037:2012** Norma que proporciona directrices de identificación, recopilación, adquisición y preservación de la evidencia digital

PAIS	**CUERPO LEGAL**	**DELITOS INFORMATICOS**	**PROTOCOLO PARA LA OBTENCION DE LA EVIDENCIA DIGITAL**
Reino de España	**Código Penal** Art. 183 ter Art. 197.1 Bis – 201 Art. 251.2.7a Art. 263-267 Art. 270 - 277 Atr.390 – 394 Art. 399	**Grooming Ciberacoso infantil** - **Acceso ilícito e interceptación ilícita (delitos contra la intimidad)** - **Estafa procesal Fraude Informático** - **Interferencia en los datos u en el sistema.** - **Delitos contra la propiedad intelectual** - **Delitos en contra de la salud publica** - **Comercialización de programas informáticos** - **Contra la honra**	**Normas internacionales** - UNE197010:2015 - UNE710505 2013 - UNE71506:2013 - ISO/IEC27037:2012 - ISO/IEC27042:2015

PAIS	**CUERPO LEGAL**	**DELITOS INFORMATICOS**	**PROTOCOLO PARA LA OBTENCION DE LA EVIDENCIA DIGITAL**
	Art. 362 – 363 Art. 400 Art. 205 - 210	- **Amenazas y coacciones.** - **Calumnias, injurias**	
México	Código Penal de Sinaloa. Art. 217 Código Penal Federal de Mx Art. 211Bis del (1) a (5) Art. 211 Art.200 Art.147. IV Art.167 II	- **Delito Informático (Pionero en su denominación)** - **Acceso Ilícito,** - **Interferencia en los datos** - **Pornografía Infantil** - **Intervención de Correo electrónico** - **Destrucción de componentes magnéticos o electromagnético**	**Protocolo De Actuación Para La Obtención Y Tratamiento De Recursos Informáticos y/o Evidencias Digitales** **Pasos** : • Identificación de la Evidencia digital • Recolección • Registro • Embalaje • Registro de cadena de custodia • Traslado y entrega para análisis • Transportación de la evidencia digital • Desembalaje

PAIS	**CUERPO LEGAL**	**DELITOS INFORMATICOS**	**PROTOCOLO PARA LA OBTENCION DE LA EVIDENCIA DIGITAL**
	Ley Fed. Del Derecho de Autor. Art. 101-102, 108-110, 114 Ley Federal de Comunicaciones.	**Propiedad Intelectual** - **Delitos en contra del Internet.** - **Delitos por medio del Internet.**	• recepción de la evidencia digital • Registro de la cadena de custodia. • Análisis e informes • Almacenamiento en el lugar de resguardo • Traslado para la presentación de los recursos informáticos y/o evidencia digital como material probatorio • Destino final
Argentina	Código Penal Art.153 Art. 153 Bis	- **Interceptación Ilícita**	**Protocolo de Actuación para la investigación**

PAIS	**CUERPO LEGAL**	**DELITOS INFORMATICOS**	**PROTOCOLO PARA LA OBTENCION DE LA EVIDENCIA DIGITAL**
	Art.183 II Art.183 II y 197 Art.292 Art. 173(16) Art. 128	- **Acceso Ilícito** - **Atentado contra la integridad de datos.** - **Atentado contra la integridad del sistema.** - **Falsedad Informática** - **Fraude o estafa Informática.** - **Pornografía infantil**	**científica en el lugar de los hechos.** Pasos previos a la recolección y preservación de la Evidencia Digital. 1. Llegar a la escena donde se va a obtener la evidencia digital 2. Acción de las Fuerzas de Seguridad o agentes que no debe alterar los datos contenidos en computadores o dispositivos de almacenamientos 3. En el caso que se tenga que acceder a los datos o información de dispositivos de almacenamiento informático, quién efectúe debe ser persona idónea 4. Auditar y registrar todo el proceso

PAIS	CUERPO LEGAL	DELITOS INFORMATICOS	PROTOCOLO PARA LA OBTENCION DE LA EVIDENCIA DIGITAL
			relativo o manipulado de la evidencia digital **Recolección de la Evidencia Digital** 1. Documentar la evidencia digital. 2. Confirmar el estado de la computadores y dispositivos informáticos 3. Fotografiar, filmar o croquis de la escena del crimen **Escenarios posibles** 1. No encender el equipo 2. Remover los cables de alimentación eléctrica de la computadora desde la parte posterior. 3. Desconectar el resto de los cables del USB y dispositivos informáticos.

PAIS	**CUERPO LEGAL**	**DELITOS INFORMATICOS**	**PROTOCOLO PARA LA OBTENCION DE LA EVIDENCIA DIGITAL**
			4. Encintar todas las entradas de puertos, cables de alimentación y otros. 5. Registrar la marca, modelo y número de serie,de computadores y sus periféricos.
Bolivia	CP. Delitos Informáticos Art.363 Bis Art.363 Ter Ley 3325 Trata y Tráfico de personas y otros delitos relacionados.	- **Manipulación Informática.** - **Alteración, acceso y uso indebido de datos informáticos.** - **Pornografía Infantil**	No considera ningún protocolo de tratamiento para la Cadena de Custodia Digital.

CAPÍTULO 3

ACUERDOS Y TRATADOS INTERNACIONALES RELACIONADOS CON LOS DELITOS INFORMÁTICOS Y LA EVIDENCIA DIGITAL

3.1 Introducción.

En el presente capítulo se busca determinar cuáles son los acuerdos y tratados internacionales relacionados con la regulación de los delitos informáticos en general y específicamente cuáles son los protocolos que se establecen para el tratamiento de la evidencia digital.

Durante el desarrollo de este capítulo se ha llegado a determinar que la base fundamental para estas temáticas es el Convenio Sobre Ciberdelincuencia de Budapest de 2001 del que se derivan todas las demás normas internacionales.

A continuación, se procede a analizar esta normativa internacional:

3.2 Convenio Sobre Ciberdelincuencia (Serie de Tratados Europeos No 185)

El Convenio sobre ciberdelincuencia número 185 forma parte de la serie de tratados europeos fue firmado el 23 de noviembre del 2001 en Hungría – Budapest, y entró en vigencia el 1 de julio de 2004; éste fue impulsado por el Consejo de Europa y otros países como los Estados miembros de la Unión Europea, junto a Estados Unidos, Canadá, Australia y Japón. Chile se incorporó tras la aprobación por parte del Congreso Nacional el 16 de noviembre de 2016. Con posterioridad, en el 2018 fue ratificado por Argentina y Colombia.

Actualmente el Convenio es el único instrumento que abarca todos los temas relacionados a la ciberdelincuencia, y es por eso que esta herramienta es tan importante. Es el acuerdo internacional de uso más extendido para desarrollar la legislación de combate al cibercrimen.

En resumen, el Convenio tiene como objetivo armonizar la legislación relativa al cibercrimen, mejorar las capacidades de investigación de estos delitos y establecer un régimen efectivo de cooperación y asistencia internacional. Entre sus principales

disposiciones destacan la obligación de tipificar delitos contra la integridad de los sistemas o datos informáticos y su contenido, y establecer procedimientos que faciliten la investigación penal. El Acuerdo resuelve también los aspectos de la cooperación y asistencia internacional en materias como extradición, acceso y consentimiento transfronterizo y el establecimiento de un equipo experto en una Red 24/7 como punto de contacto localizable las 24 horas del día. (Barrios A., 2018)

Existe además un Protocolo Adicional al Convenio sobre la penalización de actos de índole racista y xenófoba.

El carácter transnacional de la Ciberdelincuencia ha llevado a adoptar un enfoque normativo de cooperación y armonización regulatoria entre los países para enfrentar la naturaleza global del fenómeno.

El Convenio de Budapest, tiene como objetivo incrementar la eficacia de las investigaciones y procedimientos penales relativos a los delitos informáticos, así como permitir la obtención de pruebas electrónicas de los delitos, mediante una cooperación internacional reforzada, rápida y eficaz en materia penal. Otro de los objetivos es promover la armonización de la legislación que regula el cibercrimen, a nivel del derecho penal sustantivo de cada Parte; mejorar las capacidades nacionales para la investigación de este tipo de delitos, conforme al derecho procesal de cada país; y establecer un régimen ágil y efectivo de cooperación internacional principalmente para facilitar la investigación transnacional de estos delitos. (Barrios A., 2018)

La adhesión al tratado, según establece su Artículo 37, se encuentra abierta a la incorporación de países que no sean miembros del Consejo de Europa. Las medidas que deben ser adaptadas por los Estados, tanto a nivel de derecho penal sustantivo, como en materia de derecho procesal.

Respecto de la jurisdicción de las Partes para conocer y juzgar los delitos su Artículo 22 establece que cada Estado Miembro deberá adoptar las medidas que la afirmen, cuando el delito se haya cometido: a) en su territorio; o b) a bordo de un buque que enarbole su pabellón; o c) a bordo de una aeronave matriculada según sus leyes; o d) por uno de sus nacionales, si

el delito es susceptible de sanción penal en el lugar de su comisión o si ningún Estado tiene competencia territorial respecto del mismo. (Organización de los Estados Americanos, 2001)

Con relación al Derecho Penal Sustantivo, la tipificación de los delitos de acuerdo al convenio y que deberán ser sancionadas las figuras de tentativa y complicidad en los delitos tipificados Artículo 11, y exigir responsabilidad penal a las personas jurídicas Artículo 12. Asimismo, dispone que las sanciones deberán ser efectivas, proporcionadas y disuasorias, incluyendo penas privativas de libertad Artículo 13. (Organización de los Estados Americanos, 2001)

En materia del Derecho procesal penal, el Convenio dispone que cada Estado que haya firmado, ratificado o se adhiera, adoptar las medidas legislativas necesarias para establecer los procedimientos que faciliten la investigación en la persecución penal Artículo 14, así como para asegurar que garanticen la protección de los derechos humanos y las libertades personales Artículo 15°. (Organización de los Estados Americanos, 2001)

Los procedimientos que la Convención establece son:

- La conservación rápida de datos informáticos almacenados, incluido el tráfico de datos **Artículo 16**;
- La conservación y revelación parcial rápidas de los datos sobre tráfico **Artículo 17**;
- La orden a personas y proveedores de servicios de presentar la información requerida **Artículo 18**;
- El registro de todo tipo de dispositivo o sistema de almacenamiento informático y la confiscación de los datos informáticos almacenados en ellos **Artículo 19**;
- La obtención en tiempo real de datos relativos al tráfico **Artículo 20**;
- La interceptación de datos relativos al contenido de las comunicaciones **Artículo 21**.

La búsqueda de acuerdos y tratados internacionales para el presente objetivo específico ha puesto en evidencia que el **Convenio Sobre Ciberdelincuencia (Serie de Tratados**

Europeos No 185) es el instrumento internacional más detallado y específico con relación a la temática de la presente investigación, razón por la que no se pasará a desarrollar otros instrumentos ya obsoletos que pudieran haber sido parte del desarrollo de las normas internacionales de tratamiento y regulación de los delitos informáticos y la evidencia digital.

Como evidencia de lo anteriormente señalado, a continuación, se procede a caracterizar las conceptualizaciones, recomendaciones, manuales y buenas prácticas en general que están vigentes en la Organización de las Naciones Unidas, en la Organización de los Estados Americanos, así como en la Policía Internacional - INTERPOL. Todas estas inspiradas en el **Convenio Sobre Ciberdelincuencia (**Serie de Tratados Europeos No 185**).**

3.3 Organización de las Naciones Unidas (ONU)

El Manual de las Naciones Unidas sobre prevención y control de delitos informáticos, de 1994 centró su atención en el concepto de Delitos Informáticos. Con la evolución hoy en día la Organización de las Naciones Unidas hace una diferenciación entre delitos informáticos y Ciberdelitos recurre a las Tecnologías de la Información y Comunicación en particular al Internet, para la comisión de los actos delictivos de alcance transnacional y cometidos en contra o a través del uso de datos o sistemas informáticos. (UNODC, 2015, pp. 6-11)

La Organización de Naciones Unidas clasifica de distintas maneras a los tipos de Ciberdelitos conforme a variados principios;

- Fraudes mediante la manipulación de computadores Programas, datos de entrada y salida, repetición automática de procesos;
- Delitos contra elementos físicos
- Delitos contra elementos lógicos: Acceso ilícito a datos y sistemas informáticos y acceso ilícito a datos y protección de programas.
- Falsificaciones informáticas: Alteración de documentos, falsificación de documentos:
- Daños o modificaciones de programas o datos computarizados: Sabotaje, virus.

- Accesos no autorizados a servicios y sistemas informáticos: Reproducción no autorizada.
- Delitos cometidos a través de sistemas informáticos: Estafas, apoderamiento de dinero p/tarjeta de cajero, uso de correo electrónico email con finalidad criminal y utilización de internet como medio criminal. (Acurio Del Pino, 2016)

Y los Delitos Informáticos son cometidos en provecho propio, o para obtener beneficios económicos o perjudicar económicamente a otros, se tipifican mediante tipos delictivos generales no relacionados necesariamente a la informática. (UNODC, 2015)

La Organización de Naciones Unidas respecto a la Evidencia Digital refiere que son: Técnicas forenses digitales, Manejo de pruebas electrónicas y mecanismos judiciales de cooperación internacional en asuntos penales.

Evidencia Digital: Evidencia es un término que procede del latín Evidentĭa y que permite indicar una certeza manifiesta que resulta innegable y que no se puede dudar. En el derecho, una evidencia es una prueba determinante en un proceso judicial puede utilizarse para designar a aquello que permite demostrar la verdad de un hecho de acuerdo con los criterios establecidos por la ley. (UNODC, unodc.org, 2021)

Respecto al trato de Evidencia Digital mediante una técnica forense digital y manejo de pruebas electrónicas refiere que:

1. Recolección
    - Manejo de la evidencia digital; tomar en cuenta la auditabilidad, repetibilidad, reproducibilidad y justicabilidad,
    - Precaución en el lugar del incidente
2. Adquisición
    - Realización de tomas fotográficas
    - Identificación de la Evidencia Digital, una vez que esto suceda se debe *documentar* desde el momento de la recolección.
3. Aseguramiento de Evidencia Digital, para la preservación: El *Primer responsable de la Evidencia Digital* debería poder demostrar que la evidencia digital no ha sido modificada desde que fue recolectada y si lo fue, justificar el porqué de las acciones

de cambios inevitables y documentar, para luego proceder al embalaje y transporte de la evidencia digital para su almacenamiento final; el almacenamiento de la evidencia digital siempre será a través de un medio electrónico.

4. Cadena de Custodia Digital , esta debe mantenerse durante toda la vida útil de la evidencia digital.

El contenido de la *Cadena de Custodia Digital* son las siguientes:

- El registro de la cadena de custodia digital
- Identificador único de la evidencia digital
- Quién, accedió, verifico la evidencia digital

5. Ejercicios prácticos, es organizar un lugar para que con un equipo de cómputo encendido se realice tomas fotográficas para posteriormente documentarlas.

3.4 **Organización de Estados Americanos (OEA)**

El *Internet*, las redes y las TIC se han convertido en instrumentos indispensables para los Estados miembro de la OEA.

El internet ha impulsado un gran crecimiento en la economía mundial y ha aumentado la eficacia, productividad y creatividad en todo el hemisferio. Individuos, empresas y gobiernos cada vez utilizan más las Tecnologías de la Información y Comunicación que integran al Internet para hacer negocios; organizar y planificar actividades personales, empresariales y gubernamentales; transmitir comunicaciones; y realizar investigaciones.

La Organización de Estados Americanos luego de varias encuentros, reuniones y asambleas cuenta con:

Comité Interamericano contra el Terrorismo (CICTE)

1. Desarrollo de políticas: el Programa ayuda a los Estados miembros de la OEA a desarrollar estrategias nacionales de ciberseguridad que involucren a todas las partes

interesadas relevantes y se adapten a la situación legislativa, cultural, económica y estructural de cada Estado Miembro.

2. Creación de capacidades: el programa ayuda a establecer equipos nacionales de respuesta a incidentes de seguridad informática y brinda asistencia técnica personalizada y oportunidades de capacitación para fortalecer las instituciones y organizaciones nacionales. Adicionalmente, cuenta con la red, la cual rinda inteligencia sobre amenazas y tendencias cibernéticas en la región.
3. Investigación y divulgación: el programa desarrolla documentos técnicos, herramientas e informes para orientar a los responsables de la formulación de políticas, los CSIRT, los operadores de infraestructura, las organizaciones privadas y la sociedad civil, destacando los desarrollos actuales e identificando problemas y desafíos clave de ciberseguridad en la región.

Comisión Interamericana de Telecomunicaciones (CITEL)

1. Promulgar normas para tipificar como Delitos Informáticos a los abusos informáticos.
2. Comprometer el personal y los recursos adecuados
3. Mejorar las habilidades para localizar e identificar a los delincuentes
4. Mejorar las habilidades para recoger y computar pruebas a nivel internacional y regular.

Reunión de Ministros de Justicia o Ministros o Procuradores Generales de las Américas (REMJA).

El Grupo de Trabajo se reunió el 21 y 22 de enero de 2010 en la sede de la Organización en EEUU, Washington, D.C. C-018/10 y 26 de febrero de 2010 con sede en Brasil, Brasilia. C-022/2010.

El Grupo de Trabajo formulo 17 recomendaciones para fortalecer y consolidar la cooperación hemisférica en la prevención y el combate contra el delito cibernético; las recomendaciones que se pasa a resaltar por su importancia son las siguientes:

1. Que los Estados que aún no lo han hecho, en el menor plazo posible, *establezcan unidades o entidades encargadas específicamente de dirigir y desarrollar la investigación y procesamiento de delitos cibernéticos y les asignen los recursos humanos, financieros y técnicos* necesarios para el desempeño de sus funciones en forma eficaz, eficiente y oportuna.

2. Que los Estados que aún no lo han hecho, a la brevedad posible, *suministren a la Secretaría General de la OEA la información actualizada sobre las autoridades de persecución penal y de policía que sirven como puntos de contacto* para la cooperación internacional en materia de delito cibernético y pruebas electrónicas. Asimismo, que la Secretaría General de la OEA, con base en la información que reciba de los Estados, continúe consolidando y manteniendo actualizados los dos directorios de los citados puntos de contacto.

3. Que los Estados que aún no lo han hecho, en el menor plazo posible, examinen sus *sistemas jurídicos y adopten la legislación y las medidas procesales* necesarias que específicamente se requieran para tipificar las diversas modalidades de delitos cibernéticos, que aseguren la investigación y procesamiento de tales delitos en forma efectiva, eficaz y oportuna y que permitan la cooperación entre los Estados en la investigación y procesamiento de tales delitos.

4. Que los Estados que aún no lo han hecho, en el menor plazo posible, *adopten la legislación y las medidas procesales necesarias para asegurar la obtención y mantenimiento en custodia de todas las formas de pruebas electrónicas y su admisibilidad en los procesos y juicios penales* y permitir la asistencia mutua entre los Estados en los asuntos relacionados con las pruebas electrónicas, incluyendo el desarrollo de reglamentaciones para los proveedores de servicios que garanticen la preservación y recuperación de la información almacenada y de tránsito.

5. Que los Estados que aún no lo han hecho, *desarrollen e implementen estrategias nacionales de seguridad cibernética, que incluyan esfuerzos para prevenir, investigar y procesar los delitos cibernéticos*, como parte de un esfuerzo más amplio y coordinado para proteger las computadores y redes de los ciudadanos, las empresas y los gobiernos.

6. Reconocer la consideración que algunos Estados Miembros de la OEA le han dado, y recomendar *a aquellos que aún no lo han hecho a que le den la debida consideración, a la aplicación de los principios de la Convención del Consejo de Europa sobre la Delincuencia Cibernética y la adhesión a la misma, así como a la adopción de las medidas legales y de otra naturaleza que sean necesarias para su implementación*, teniendo en cuenta las recomendaciones adoptadas por este Grupo de Trabajo y por las REMJA en sus últimas reuniones. Asimismo, que, con estos propósitos, se continúen realizando actividades de cooperación técnica con el auspicio de la Secretaría General de la OEA y el Consejo de Europa.

7. Continuar fortaleciendo los mecanismos que permitan el intercambio de información y la cooperación con otras organizaciones e instancias internacionales en materia de delito cibernético, tales como el Consejo de Europa, las Naciones Unidas, la Unión Europea, el Foro de Cooperación Económica del Pacífico Asiático (APEC), la Organización para la Cooperación y el Desarrollo Económicos (OCDE), el G-8, el Commonwealth y la INTERPOL, de manera que los Estados Miembros de la OEA puedan aprovechar los desarrollos dados en dichos ámbitos.

8. Que, como parte de los esfuerzos dirigidos a facilitar y consolidar la cooperación para prevenir, investigar y sancionar los delitos cibernéticos, los Estados *fomenten, aún más, las relaciones entre las autoridades responsables de la prevención, investigación y procesamiento de tales delitos y el sector privado, especialmente con aquellas empresas proveedoras de servicios de tecnología de la información y las comunicaciones, en particular de servicios de "Internet".*

A continuación, algunas de las 23 de las más importantes recomendaciones del REMJA del 29 de abril de 2022 del Grupo de Trabajo en Delito Cibernético de las REMJA-XI (documento REMJA-XI/DOC.2/21 rev. 1) y la Resolución AG/RES. 2975 (LI-O/21) de la Asamblea General de la OEA:

1. Que los Estados que aún no lo han hecho, en el menor plazo posible, establezcan unidades o entidades encargadas específicamente de dirigir y desarrollar la

investigación y procesamiento de delitos cibernéticos y les asignen los recursos humanos, financieros y técnicos necesarios para el desempeño de sus funciones en forma eficaz, eficiente y oportuna.

2. Que la Secretaría Técnica de las REMJA (Departamento de Cooperación Jurídica de la Secretaría de Asuntos Jurídicos de la OEA) continúe consolidando y manteniendo actualizado el directorio de las autoridades designadas por los Estados que sirven como puntos de contacto para la *cooperación internacional en materia de delito cibernético y evidencias electrónicas* y que, con este propósito, los Estados que aún no lo han hecho, a la brevedad posible, le suministren dicha información actualizada.
3. Que los Estados que aún no lo han hecho, en el menor plazo posible, *examinen sus sistemas jurídicos y adopten o actualicen la legislación y las medidas procesales* necesarias que específicamente se requieran para tipificar las diversas modalidades de delitos cibernéticos, que aseguren la investigación y procesamiento de tales delitos en forma efectiva, eficaz y oportuna y que permitan la cooperación entre los Estados en el marco de esas mismas actividades.
4. Que los Estados que aún no lo han hecho, en el menor plazo posible, *adopten o actualicen la legislación y las medidas procesales necesarias para asegurar la obtención y mantenimiento en custodia de todas las formas de evidencias electrónicas y su admisibilidad en los procesos y juicios penales*. Así mismo, que en el menor tiempo posible adopten las medidas legales correspondientes para permitir la asistencia mutua entre los Estados en los asuntos relacionados con las evidencias electrónicas.
5. Que los Estados que aún no lo han hecho, en el menor plazo posible, *procuren adoptar legislación para asegurar la recolección y custodia de todas las formas de pruebas electrónicas* para que los proveedores de servicios garanticen la preservación y recuperación de la información almacenada o de tránsito, cuando sea solicitado.
6. Que los Estados que aún no lo han hecho, *desarrollen e implementen estrategias nacionales que incluyan esfuerzos para prevenir, investigar y procesar los delitos cibernéticos, así como el desarrollo de principios clave para la incorporación de la perspectiva de género y la inclusión en los esfuerzos para fortalecer las capacidades en materia de delincuencia cibernética*. Lo anterior como parte de un esfuerzo más

amplio y coordinado para proteger los sistemas de información y redes informáticas de los ciudadanos, las empresas y los gobiernos.

7. Recomendar a los Estados Miembros de la OEA que no lo hayan hecho *que consideren adherir al Convenio sobre la Ciberdelincuencia del Consejo de Europa y adoptar las medidas legales y de otro tipo necesarias para su implementación, así como participar y contribuir en el desarrollo de instrumentos internacionales para el combate y prevención del ciberdelito*. Asimismo, que, con estos propósitos, se continúen realizando actividades de cooperación técnica con el auspicio de la Secretaría Técnica de las REMJA y el Consejo de Europa.
8. Continuar fortaleciendo los mecanismos que permitan el intercambio de información y la cooperación entre la REMJA y otras organizaciones internacionales en materia de delito cibernético, tales como las Naciones Unidas, el Consejo de Europa, la Unión Europea, el Foro de Cooperación Económica Asia-Pacífico (APEC), la Organización para la Cooperación y el Desarrollo Económicos (OCDE), el G-7, el Commonwealth y la INTERPOL, de manera que los Estados Miembros de la OEA puedan aprovechar los desarrollos dados en dichos ámbitos.
9. Que, como parte de los esfuerzos dirigidos a facilitar y *consolidar la cooperación para prevenir, investigar y sancionar los delitos cibernéticos*, los Estados continúen fomentando de forma conjunta, aún más, las relaciones entre las autoridades responsables de la prevención, investigación y procesamiento de tales delitos y el sector privado, especialmente con aquellas empresas proveedoras de servicios de tecnología de la información y las comunicaciones, en particular de servicios de Internet, con el fin de agilizar y mejorar la obtención de información en el contexto de los procedimientos de asistencia mutua en el marco del respeto de las legislaciones internas.
10. Que los Estados que aún no lo han hecho adopten las medidas necesarias con el fin de que puedan contar con estadísticas sistematizadas anualmente en materia de investigación, persecución y sanción de los delitos cibernéticos, así como de las solicitudes de asistencia mutua enviadas y recibidas y su resultado. Asimismo, que los Estados que aún no lo han hecho, le asignen a una entidad la responsabilidad de

compilar las estadísticas antes referidas e informen a la Secretaría Técnica de las REMJA los datos de contacto de dicha entidad.

11. Que el Grupo de Trabajo en Delito Cibernético de las REMJA se continúe consolidando como foro hemisférico para el intercambio de *buenas prácticas* entre los Estados Miembros de la OEA en *materia de investigación, persecución y sanción de los delitos cibernéticos y manejo de evidencia digital.*
12. Facilitar el conocimiento en el marco del proceso de las MISPA (Reuniones de Ministros en Materia de Seguridad Publica de las América), de los desarrollos dados, en las REMJA y su Grupo de Trabajo en Cooperación Jurídica contra los Delitos Cibernéticos, para el fortalecimiento de la cooperación hemisférica en el combate de tales delitos, de manera que ellos puedas ser tenidos en cuenta y aprovechados, en lo que sea pertinente, por las autoridades de los Estados Miembros que participan en la MISPA.
13. Que el Grupo de Trabajo se reúna con antelación a la REMJA XIII con el fin de considerar, entre otros, los avances dados en la implementación de las presentes recomendaciones.

Evidencia Digital .- La evidencia digital, es todo registro informático almacenado en un dispositivo informático o que se transmite a través de una red informática y que pudiera tener valor probatorio para una investigación (Martin Nessi, 2017)

Cano, quien nos manifiesta que la evidencia digital es un tipo de evidencia física. Continúa definiendo a la misma como aquella evidencia que está construida por campos magnéticos y pulsos electrónicos que pueden ser recolectados y analizados con herramientas y técnicas especiales. (José Alejandro Mosquera González - Andrés Felipe Certain Jaramillo - Jeimy J. Cano, 2005)

La *Evidencia Digital* es aquel archivo o conjunto de archivos electrónicos contenidos en un dispositivo físico que se pueden encontrar en el campo sujeto a análisis, o que se localizan remotamente, como es el caso de la información almacenada en internet. Esta evidencia se compone de un cúmulo de mensajes de datos que pueden estar en cualquier formato. (Ramos Álvarez, Benjamin Ribagorda Garnacho, Arturo, 2004)

Las recomendaciones que se debe seguir para la obtención optima de la a la Evidencia Digital son las siguientes:

- Investigación: Técnicas de análisis de la evidencia digital, como combinar métodos de investigación tradicional con Tecnologías de la Información y Comunicación.
- Persecución: Como preservar la evidencia digital en una Corte Judicial.
- Evaluación y Análisis: Como analizar la evidencia digital que es presentada y como asegurarse de que la misma no ha sido alterada y como conectar leyes existentes con crímenes modernos.
- Uso del Manual del Manejo de la evidencia digital.

3.5 **Policía Internacional - INTERPOL**

Como referencia a la 6ª Conferencia Internacional Sobre Ciberdelincuencia realizada en el Cairo (Egipto), el 13 al 15 de abril de 2005, recomendó a todos los países miembros:

La utilización del Convenio sobre Ciberdelincuencia del Consejo de Europa como referencia en materia de normas internacionales procedimentales y legales mínimas para la lucha contra la ciberdelincuencia. Se instará a los países a suscribirlo. Este Convenio se distribuirá a todos los países miembros de INTERPOL en los tres idiomas oficiales. (Acurio Del Pino, 2016, p. 49)

- INTERPOL aumente sus esfuerzos dentro de la iniciativa sobre formación y normas operativas con objeto de proporcionar unos estándares internacionales para la búsqueda, el decomiso y la investigación de pruebas electrónicas.
- Que la formación y la asistencia técnica sigan considerándose prioritarias en la lucha internacional contra la ciberdelincuencia, incluidas la preparación de los cursos adecuados y la creación de una red internacional de escuelas de formación y de instructores, lo que implica el uso óptimo de herramientas y programas tales como los cursos itinerantes INTERPOL y los módulos de enseñanza en línea. Las iniciativas de formación y asistencia técnica deben ser transversales, y en ellas deben participar los sectores públicos y privado, entre las que figuran las universidades.

- Que se inicie y desarrolle la esencial cooperación y comunicación con instituciones supranacionales, como pueden ser las Naciones Unidas, y con entidades nacionales dedicadas a la lucha contra la ciberdelincuencia, y se impulse una respuesta rápida.
- Que la información relativa a casos de ciberdelincuencia se recopile en la base de datos de INTERPOL y se transmita en forma de resultados analíticos, a fin de ayudar a los países miembros a adoptar las estrategias de prevención apropiadas.
- Que se creen grupos de trabajo de INTERPOL sobre delincuencia informática en las regiones donde actualmente aún no existen. Los conocimientos adquiridos por los grupos de trabajo ya constituidos deberán utilizarse para apoyar la creación de los nuevos.
- Que la Secretaria General de INTERPOL organice una conferencia en la que participen, entre otros, representantes de los distintos organismos que trabajan en el ámbito de la justicia penal, a fin de determinar un marco para la cooperación en materia de lucha contra la ciberdelincuencia.
- Que INTERPOL encabece la promoción de estas recomendaciones, que son esenciales para combatir eficazmente la delincuencia informática y proteger a los ciudadanos de todo el mundo en el ciberespacio.
- Que INTERPOL, realiza un análisis forense para extraer datos contenidos en las pruebas electrónicas o la *Evidencia Digital,* transfórmalas en información de utilidad operativa y presentar las conclusiones con miras a la persecución penal. (Interpol, 2022)

CAPÍTULO 4

NECESIDAD DE INCLUIR EL USO ALGORÍTMICO EN LA BUSQUEDA DE LA EVIDENCIA DIGITAL COMO PRUEBA IRREFUTABLE PARA LA AVERIGUACIÓN DE LA VERDAD MATERIAL EN ACCIONES ANTIJURÍDICAS EN LAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

4.1 Análisis Sociológico – Jurídico.

4.1.1 Introducción.

En sentido general, la sociología del derecho tiende a considerar al derecho como un *fenómeno social*, esto es, como un objeto de estudio de la ciencia social encuadrable en el *hecho social* identificado por Durkheim, y, por lo tanto, en relación con otros hechos sociales tales como los antes mencionados, y todos los que pudieran ser identificados en cualquier sociedad.

Puede concluirse que la sociología jurídica es una rama más del derecho, pero también lo es de la sociología, la cual vislumbra los entramados sociales bajo los cuales crecen o se originan las leyes que nos rigen. (Fucito, 1989)

La Tipología Sociológica jurídica.

Un estudio socio-jurídico que ignore y no tome en consideración las complejas construcciones normativas e institucionales, puede aparecer lleno de imperfecciones y hasta de errores elementales que lo hagan inutilizable para los juristas (Diaz 1998, pag.169).

Por ello si bien el estudio será de corte socio-jurídico, es imposible prescindir terminantemente del aspecto normativo.

Primero, una entrevista, una técnica de investigación cualitativa que consiste en hacer preguntas para conversar con los encuestados y recopilar datos sobre un tema.

De las diferentes formas de entrevistas el presente trabajo de investigación ha utilizado la entrevista semiestructurada.

4.1.2. Entrevistas semiestructuradas.

Las entrevistas semiestructuradas ofrecen al investigador un margen de maniobra considerable para sondear a los encuestados y tiene como fin recolectar una determinada información u opinión basada en la experiencia.

Además de mantener la estructura básica de la entrevista. Incluso si se trata de una conversación guiada entre investigadores y entrevistados, existe flexibilidad.

Teniendo en cuenta la estructura, el investigador puede seguir cualquier idea o aprovechar creativamente toda la entrevista.

Ventajas de las entrevistas semiestructuradas

- Las preguntas de las entrevistas semiestructuradas se preparan antes de programar la entrevista, lo que da tiempo al investigador para preparar y analizar las preguntas.
- En cierta medida es flexible, al mismo tiempo que mantiene las directrices de la investigación.
- Los investigadores pueden expresar las preguntas de la entrevista en el formato que prefieran, a diferencia de la entrevista estructuradas

A través de estas entrevistas se pueden recopilar datos cualitativos fiables; los datos que se expresan en forma de palabras o textos que ayudan a comprender ciertas acciones y actitudes de los encuestados que no son cuantificables, por lo que su uso es muy importante para fundamentar cualquier investigación seria. (QuestionPro, 2022)

4.1.3 Diseño de los Instrumentos.

Los instrumentos utilizados en el presente trabajo fueron dos cuestionarios validados previamente con profesionales en Ingeniería de Sistemas y Abogados penalistas y se han tenido respuestas coherentes con relación a las preguntas planteadas razón por la que puede afirmarse que son útiles para conseguir el objetivo de investigación deseado.

Instrumento 1. Cuestionario a Ingenieros de Sistemas e Informáticos forenses

Pregunta 1. ¿Considera usted que la Evidencia Digital es una prueba irrefutable de la existencia de una vulneración relacionada a las Tecnologías de la Información y Comunicación si, no, por qué?

Pregunta 2. ¿Tiene algo más que agregar a la presente investigación que tiene como objetivo "Exponer la necesidad de incluir el uso algorítmico en la búsqueda de la Evidencia Digital como prueba irrefutable para la averiguación de la verdad material en acciones antijuridicas en las Tecnologías de la Información y Comunicación?

A continuación, las respuestas de los expertos en Ingenieros de Sistemas e Informáticos forenses Derecho.

Entrevista 1.

M.Sc. Elizabeth Pommier

Docente Universidad Católica Bolivia

Docente Post Grado de la Carrera de Informática Universidad Mayor de San Andrés

Respuesta 1

En general se puede tener evidencia de manipulación de evidencia en caso de que existiera, sin embargo, con el avance de la tecnología a veces se puede vulnerar esto, por ejemplo, cuando se utiliza una máquina para descargar archivos y no se puede dar con la IP por utilizar espejos en varios servidores, que van cambiando de pin. En un

ámbito más legal, se utiliza la metodología de informática forense para el levantamiento de evidencia por peritos informáticos.

Respuesta 2

Cuando se utiliza tecnología siempre debe considerarse un margen de error, incluso en los algoritmos si bien dan solución se debe realizar las pruebas necesarias para ver las vulnerabilidades que se pueden tener, sin duda un algoritmo ayudaría en la averiguación de la verdad material en acciones antijurídicas, pero se debe considerar todas las variables involucradas.

Espero haber ayudado

Entrevista 2

M.Sc. Irma Prado
Docente universitaria Universidad Mayor de San Andrés -Universidad Católica Boliviana
Ex directora de Carrera de Ingeniería de Sistemas, Universidad

Ex directora de Carrera de Ingeniería Eléctrica, Universidad Mayor de San Andrés.

Respuesta 1

La evidencia digital si puede ser una prueba irrefutable de la existencia de una vulneración relacionada con las tecnologías de la Información y comunicación, siempre y cuando esta evidencia digital sea producto de procesos idóneos. ¿Por qué?

Porque la evidencia digital podría estar mañosamente armada. Creo que primero se debe demostrar la idoneidad de la evidencia.

Respuesta 2

Creo que se debe ver la calidad del algoritmo, qué y como lo hace, luego de aprobar la calidad, sí puede ser una prueba irrefutable de la existencia de una vulneración relacionada con las tecnologías de la Información y comunicación.

Entrevista 3

M.Sc. Paola Carranza Bravo

Docente Universidad Católica Boliviana

Respuesta 1

Considero que sí es una prueba irrefutable, pues la vulneración (cambio) se puede advertir en el análisis algorítmico lógico, la referencia de la lógica se considera como la matemática filosófica que es irrefutable por esencia. Es de esta manera que la evidencia digital pasa por un escaneo figurativamente hablando, para ver, identificar y rechazar los cambios y manipuleos.

Respuesta 2

Un algoritmo es una secuencia de pasos lógicos, coherentes y finitos que no desvían el cambio a la verdad, la ciencia matemática es un campo muy cercano a la exactitud de los datos, así que cuando se piensa en relacionar la matemática con el Derecho, se está pensando en el bien.

A continuación, las respuestas de los abogados expertos en derecho informático y abogados penalistas.

Pregunta 1. ¿Cuál es el valor probatorio de un informe pericial emitido por un informático forense de un proceso judicial en el que se busca probar la realización de un ilícito relacionado con las Tecnologías de Información y Comunicación?

Pregunta 2. ¿Qué modificaciones sugiere deban ser agregadas al ordenamiento jurídico o a la formación de los operadores de justicia para mejorar el proceso de investigación de ilícitos relacionados con las Tecnologías de la Información y Comunicación?

Pregunta 3. ¿Tiene algo más que agregar que considere pueda aportar a la presente investigación que tiene como objeto de exponer la necesidad de incluir el uso

algorítmico como prueba irrefutable para la averiguación de la verdad material en acciones antijurídicas en las Tecnologías de la Información y Comunicación?

Entrevista 1

Dr. Gonzalo Contreras

Docente Universidad Católica Boliviana

Docente Universidad de La Salle

Penalista independiente en ejercicio.

Respuesta 1

Como toda pericia, la pericia informática le sirve al juez o tribunal para generar certeza y fundar su decisión en los límites racionales de la sana crítica, puesto que la pericia le permite al administrador de justicia hallar un elemento probatorio desconocido o para valorar un determinado elemento de prueba. En ese sentido, dependerá en cada caso en concreto el valor que el juez o tribunal le otorgue al peritaje informático, sea para descubrir o valorar un elemento de prueba preexistente.

Respuesta 2

En consideración a la situación actual producto de la pandemia, en la que las tecnologías han cobrado mayor relevancia, y en consecuencia toda la población realiza un mayor uso de dichas tecnologías, también se ha intensificado la comisión de hechos ilícitos dando inclusive lugar a la generación de nuevas formas ilícitas, razón por la que será importante considerar la especialización de jueces, fiscales e investigadores en el derecho de las tecnologías, generando una jurisdicción especial y unidades especiales de fiscales e investigadores.

Respuesta 3

Debido a la masificación del uso de las tecnologías y su renovación constante es necesario que el Instituto de Investigaciones Forenses fortalezca la unidad informática no solo en cuanto a los recursos humanos sino en cuanto al equipamiento que permita realizar las pericias con la mayor precisión posible.

Entrevista 2

Abog. Mst. Ariel Agramont

Abogado MCA 5476

WhatsApp: 591 772 94911

La Paz - Bolivia

Sudamérica

Respuesta 1

Un informe pericial informático realizado en las condiciones y requisitos exigidos legalmente es un elemento probatorio cuya valoración está sujeta a lo que regula el Código de Procedimiento Penal vigente: ARTÍCULO 173. (Valoración).- El juez o tribunal asignará el valor correspondiente a cada uno de los elementos de prueba, con aplicación de las reglas de la sana crítica, justificando y fundamentando adecuadamente las razones por las cuales les otorga determinado valor, en base a la apreciación conjunta y armónica de toda la prueba esencial producida.

Respuesta 2

Siempre será importante que se puedan formar en Derecho Informático para comprender los alcances regulatorios y su aplicabilidad en los casos.

Respuesta 3

No muchas gracias.

Entrevista 3

Abog. Mst. Juan José Tapia Suxo

Abogado MCA 10621

WhatsApp: 591 77707755

La Paz – Bolivia

Respuesta 1

Tiene pleno valor probatorio, en tanto y en cuanto, el perito forense informático, reconocido y acreditado por la institución correspondiente, para que esta manera sea considerada ante la autoridad jurisdiccional.

Respuesta 2

Deben de establecer la categoría de delitos y establecer las sanciones, ampliando su espectro de aplicación pues este delito tiene inclusive carácter internacional, ya que estos delitos se cometen usando recursos tecnológicos.

Respuesta 3

Establecer una entidad u oficina especifica que se dedique a la investigación de estos delitos.

Análisis de las respuestas obtenidas.

En el presente trabajo de investigación se ha utilizado la entrevista semiestructurada que ha sido validada para poder utilizarla con los expertos en el área.

Los resultados obtenidos del primer cuestionario realizado a expertos en informática forense e ingeniería de sistemas fueron los siguientes:

Se puede decir que los tres expertos coinciden en que sí es posible que la *Evidencia Digital* pueda ser considerada irrefutable siempre y cuando ésta haya sido obtenida con el procedimiento adecuado y se demuestre de esta forma su idoneidad. Asimismo, los expertos coinciden en que la informática forense es el procedimiento idóneo para la obtención de la evidencia digital.

Finalizando el cuestionario los expertos recomendaron e hicieron hincapié en las siguientes consideraciones:

A momento de diseñar un algoritmo, se debe tener especial consideración en eliminar los posibles errores humanos que pudieran dar lugar a posibles vulnerabilidades que pudieran quitar el carácter de irrefutable a la evidencia digital.

Asimismo, uno de los expertos consideró que la asociación de la ciencia matemática, en este caso representada por un algoritmo, combinada con la ciencia el derecho constituye una alianza encaminada a el bienestar de la sociedad.

Los resultados obtenidos en el cuestionario realizado a expertos en derecho informático fueron los siguientes:

Todos los expertos coinciden que, si bien existe la pericia como prueba en la normativa de nuestro país, su valor probatorio depende de la decisión de los administradores de justicia, es decir, depende su sana crítica.

Asimismo, los expertos coinciden en que es necesario capacitar a jueces, fiscales e investigadores en el derecho informático, en las Tecnologías de la Información y Telecomunicación para poder comprender adecuadamente cómo se dan estos ilícitos y las formas idóneas de identificar a sus autores

Para finalizar, los abogados penalistas consideraron importantes que debe fortalecerse el área de la informática, no solo en el recurso humano especializado sino también en el equipamiento que le permita al personal del Instituto de Investigaciones Forenses realizar pericias con la mayor precisión posible.

4.1.4. Revisión de literatura científica especializada que pone en evidencia la necesidad de utilizar un protocolo para el abordaje de la evidencia digital que incluya el uso algorítmico en Bolivia.

En los países de la región existen en la actualidad protocolos, manuales y estándares para la captura, recolección, análisis e interpretación de la evidencia digital en la comisión de delitos informáticos. El objetivo de analizar el estado actual de las investigaciones sobre la obtención de la evidencia digital es para obtener con claridad la necesidad de incorporar un procedimiento aún más avanzado a nivel Latinoamérica.

De la revisión bibliográfica se realizó una búsqueda bibliográfica manual entre las referencias de los estudios seleccionados y en diferentes bibliotecas.

Revista PGI 1, 2014 (Cruz, 2014)

Cruz Vela, Erika Marilyn

Modelo para el Análisis y Gestión de Riesgos en Fases carentes de Técnicas Herramientas Caso Tratamiento de la Evidencia Digital en el Entorno del software libre utilizando procesos unificados. (Cruz, 2014)

Las estadísticas en la comisión de delitos informáticos en Bolivia fueron las siguientes:

Entre 2003 y 2007, 185 denuncias de manipulación informática y de alteración, acceso y uso indebido de datos en toda Bolivia, pero se desconoce si alguna de ellas que resuelta.

Los datos de la Fuerza Especial de Lucha Contra el Crimen (FELCC) revelan que en Santa Cruz, La Paz y Cochabamba se producen más delitos informáticos desde 2003.

El 2007, se registró un total de 185 fraudes electrónicos en todo el país, de éstos, 177 corresponden a *Manipulación Informática* y ocho a *Alteración, Acceso Y Uso Indebido De Información*.

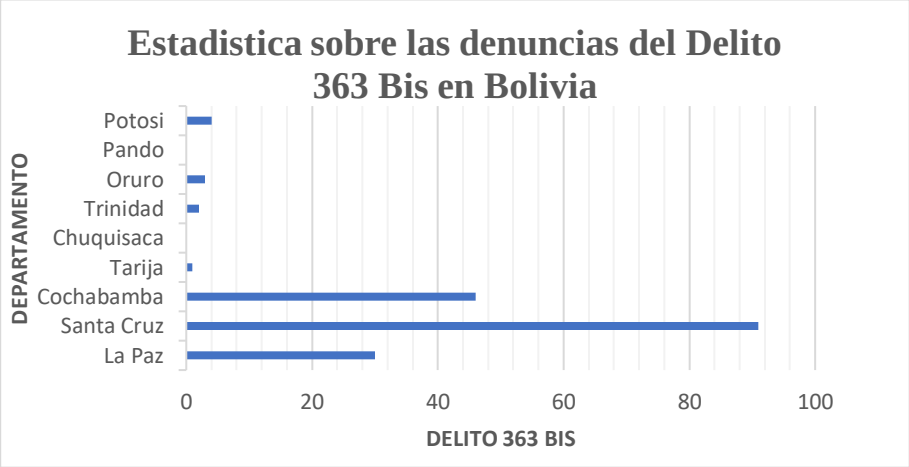


Gráfico 1: Construcción Propia en base a los datos del autor (Cruz, 2014)

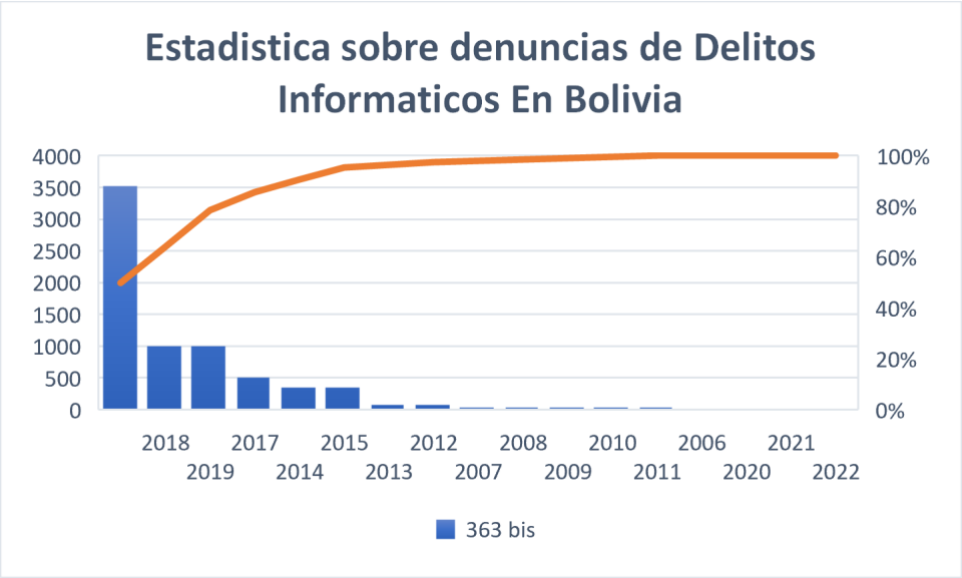


Gráfico 2. Construcción propia en base a los datos del autor (Cruz, 2014)

El grafico 3 refleja otra información interesante es conocer que:

1. 91 casos se dieron en Santa Cruz,
2. 46 en Cochabamba,
3. 30 en La Paz,
4. cuatro en Potosí,
5. tres en Oruro,
6. dos en Beni y
7. uno en Tarija.

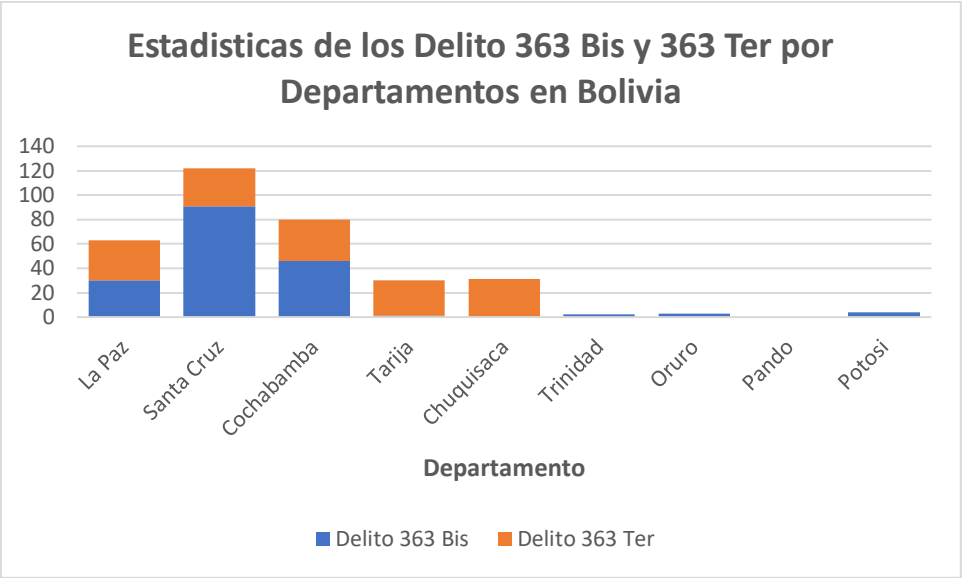


Gráfico 3. Construcción Propia en base a los datos del autor (Cruz, 2014)

Entre enero y septiembre de 2014 la comisión de delitos de alteración, acceso y uso indebido de información informática, tres ocurrieron en La Paz, dos en Cochabamba, dos en Beni y uno en Santa Cruz en contra peso de las 50 denuncias de manipulación electrónica; 27 en Santa Cruz, 12 en La Paz, nueve en Cochabamba y dos en Chuquisaca y ninguna acerca de alteración.

De 2002 a 2011, los juicios por delitos informáticos crecieron en 890%, de ocho a 79, de los cuales 62 están referidos a manipulación informática y 17, a la alteración, acceso y uso indebido de datos informáticos.

Aparte, en esta década, los juzgados paceños recibieron 228 causas referidas al primer delito y 15 del segundo.

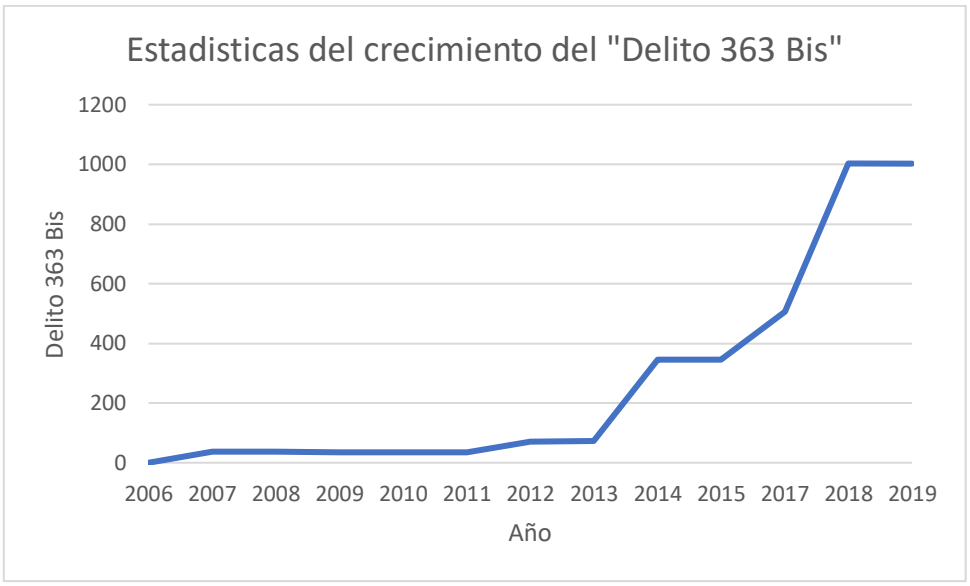


Grafico 4. Construccion Propia en base a datos del autor (Cruz, 2014)

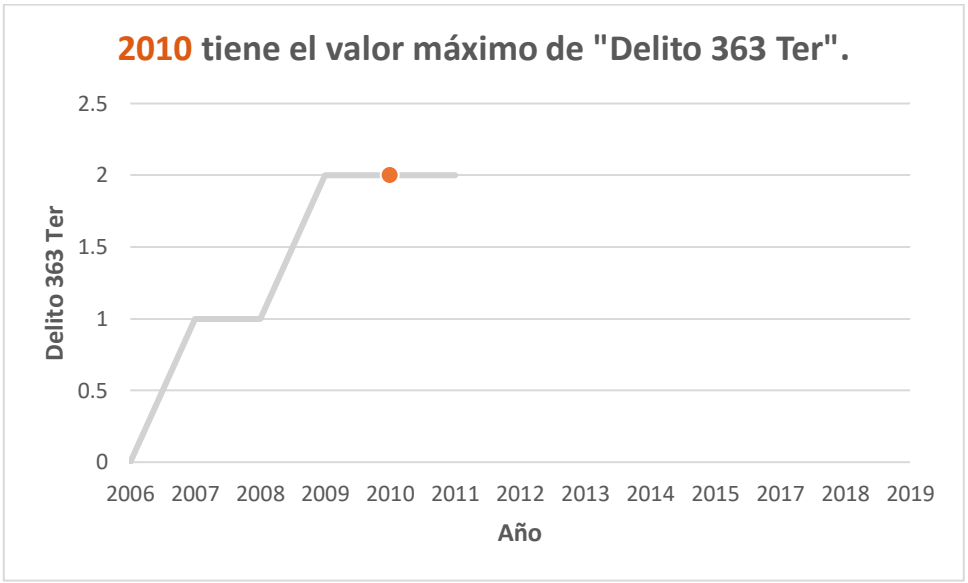


Gráfico 5. Construcción Propia en base a datos del autor (Cruz, 2014)

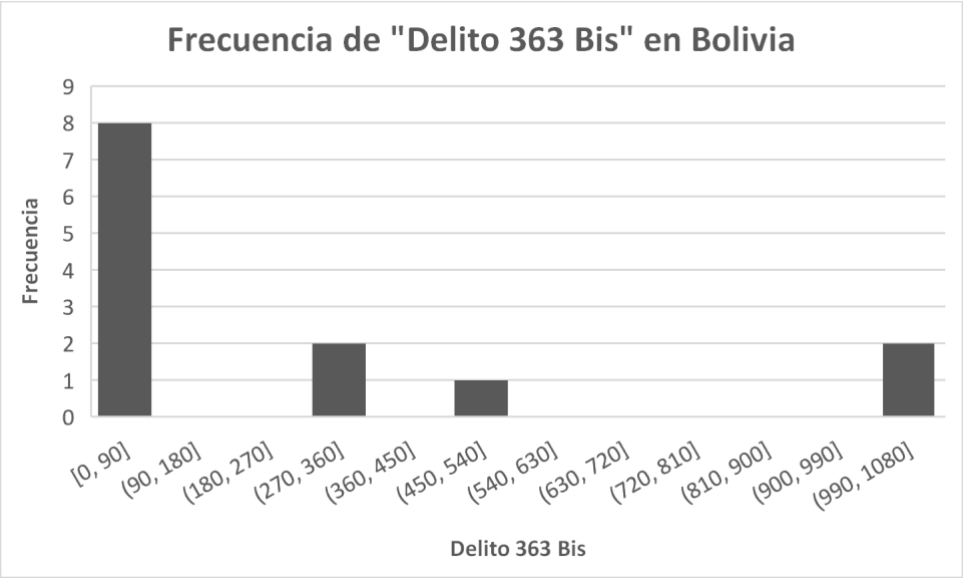


Gráfico 6. Construcción Propia en base a datos del autor (Cruz, 2014)

Revista PGI, 2021

Universidad Mayor de San Andrés La Paz - Bolivia

Francachs Castro, Bismarck (Francachs Castro, 2021)

Modelo Para Tratamiento Forense de Incidentes Informáticos en la Nube (Francachs Castro, 2021)

Este articulo propone la elaboración de un algoritmo matemático luego de haber identificado como problema la ausencia de normas o leyes para la pericia forense orientada a la Nube en Bolivia.

Los datos presentes son sobre los cambios ocurridos en el uso de herramientas de las Tecnologías de la Información y Comunicación hasta llegar a la utilización de la informática forense para la obtención de evidencias digitales en la comisión de los delitos informáticos en el uso del *Internet.*

La Tabla refleja los avances del uso de las diferentes herramientas utilizadas a cada década hasta llegar a la Informática forense. En 1984 el CART Equipo de Respuesta y Análisis Informático. 1993 se crean los principios internacionales y los procedimientos relacionados a la evidencia digital. En el año 2000 el FBI crea le

primer laboratorio forense. El RFC 3227 (Directrices para la recopilación de evidencias y su almacenamiento), la norma ISO/IEC 27037:2012

ISO/IEC: 27042:2015 (Guía para el Análisis e Interpretación de Evidencia Digital).

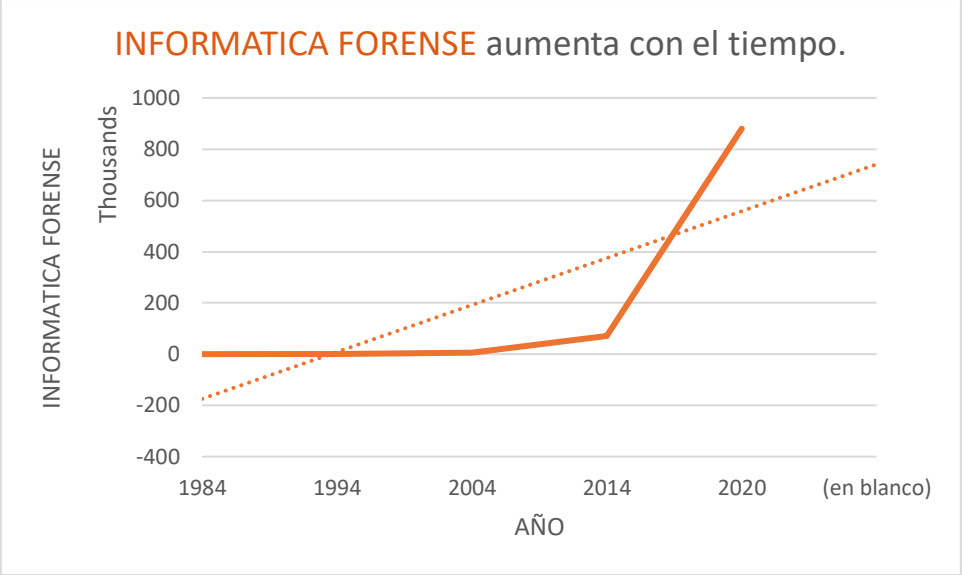


Gráfico 1. Construcción Propia en base a datos del autor (Francachs Castro, 2021)

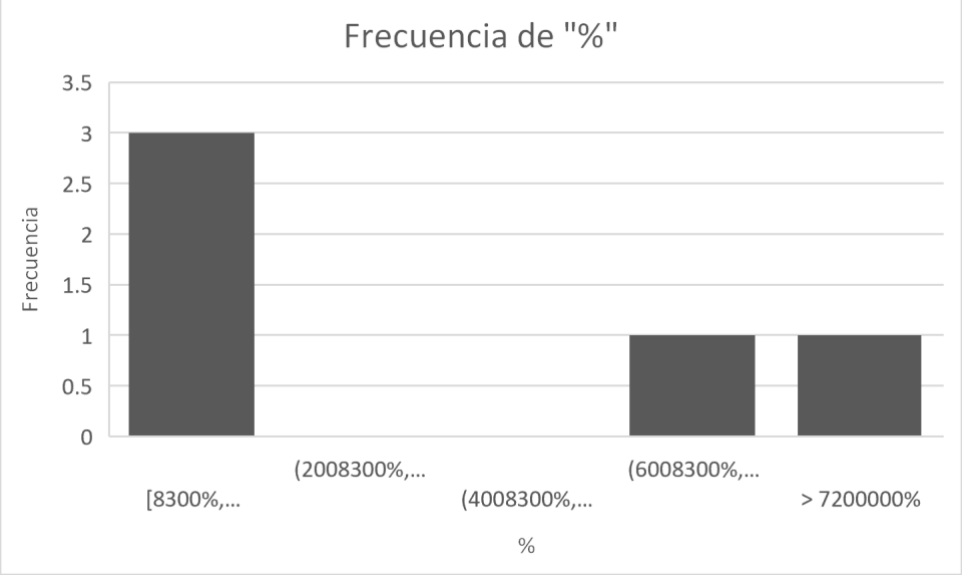


Gráfico 2. Construcción Propia en base a datos del autor (Francachs Castro, 2021)

Revista de Derecho en la Facultad de Ciencias Jurídicas y Sociales
Universidad Nacional del Litoral
Santa Fe Argentina
Temperini, Marcelo Gabriel Ignacio
Doctorando
Delitos Informáticos en Latinoamérica: Un estudio de derecho comparado. (Temperi, 2013)

La tabla refleja la estadística en porcentaje de los delitos informáticos sin sanción penal en los países de Latinoamérica.

Delito Informático %
Acceso Ilícito 19%
Interceptación Ilícita 33%
Atentado contra la integridad de los datos 14%
Atentado contra la Integridad del sistema 33%
Abuso de los dispositivos 71%
Falsedad Informática 57%
Fraude o Estafa Informática 48%
Pornografía Infantil 19%

Tabla1. Elaboración del autor (Temperi, 2013)

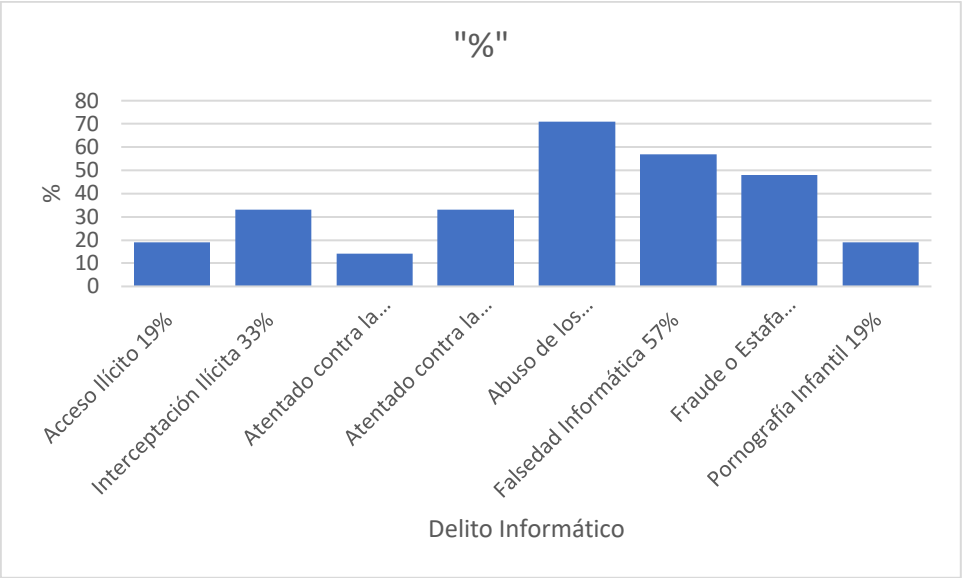


Gráfico 1: Construcción Propia en base a datos del autor (Temperi, 2013)

Estadísticas que expresan el nivel de sanción penal de los delitos analizados, por país.

País %
Argentina 88%
Bolivia 50%
Brasil 63%
Chile 63%
Colombia 75%
Costa Rica 88%
Cuba 0%
Ecuador 63%
El Salvador 63%
Guatemala 50%
Haití 0%
Honduras 50%
México 75%
Nicaragua 0%
Panamá 88%

Paraguay 88%
Perú 63%
Puerto Rico 100%
República Dominicana 100%
Uruguay 63%
Venezuela 100%

Tabla 2. Elaboración del autor (Temperi, 2013)

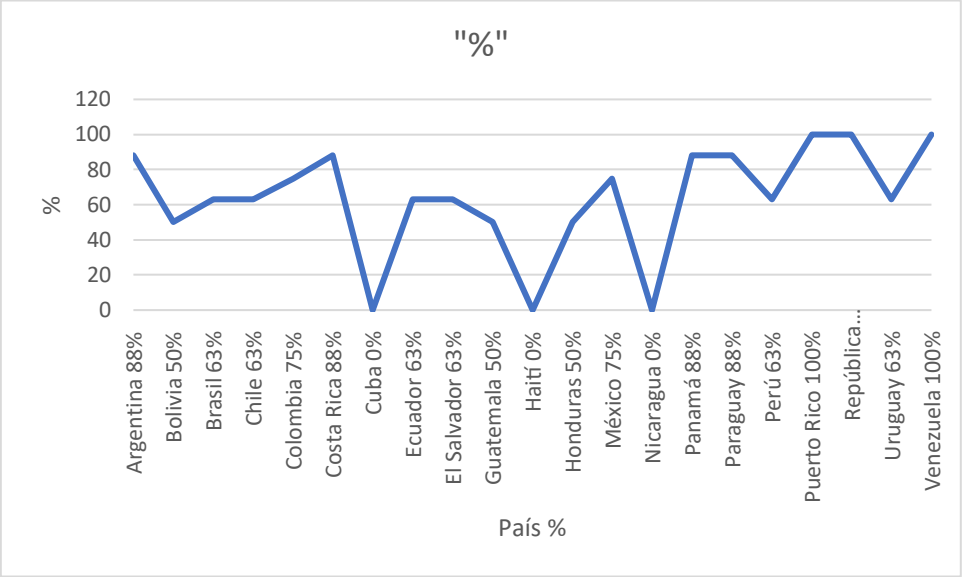


Gráfico 2: Construcción Propia en base a datos del autor (Temperi, 2013)

Ranking de países con menor sanción penal para los delitos informáticos considerados.

País %
Puerto Rico 100%
República Dominicana 100%
Venezuela 100%
Argentina 88%
Costa Rica 88%
Panamá 88%
Paraguay 88%
Colombia 75%
México 75%
Brasil 63%
Chile 63%
Ecuador 63%
El Salvador 63%
Perú 63%
Uruguay 63%
Bolivia 50%
Guatemala 50%
Honduras 50%
Cuba 0%
Haití 0%
Nicaragua 0%

Tabla 3. Elaboración del autor (Temperi, 2013)

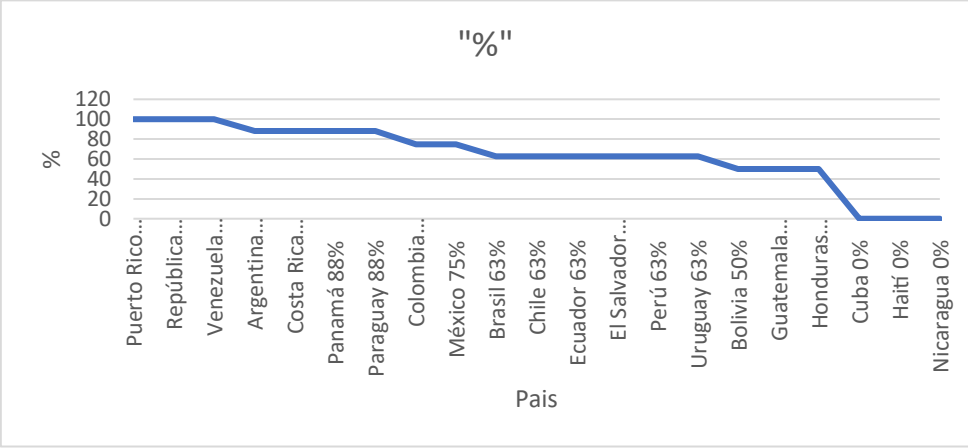


Gráfico 3: Construcción Propia en base a datos del autor (Temperi, 2013)

De la revisión de los artículos de revistas científicas bolivianas y el estudio estadístico de los delitos informáticos en Latinoamérica del doctorando Marcelo Temperi, se puede demostrar la necesidad urgente que tiene Bolivia de avanzar en relación a los delitos que suceden y que el uso algorítmico para optimizar la averiguación de la verdad material en la comisión de las acciones antijuridicas cometidas en las Tecnologías de la Información y Comunicación.

CONCLUSIONES Y RECOMENDACIONES

Conclusión al objetivo específico 1 “Estudiar la legislación comparada acerca del tratamiento y regulación de los Delitos Informáticos y la Evidencia Digital “

De la legislación revisada de los países estudiados se concluye que: Argentina es el país más avanzado en su legislación respecto a *Delitos Informáticos*. Se adhirió al Convenio de Budapest de 2001 en 2010 y lo ratificó en 2017. Dicho convenio es el referente, más completo sobre la Ciberdelincuencia. Si bien, la normativa argentina, no tiene una adecuación plena, se puede decir que su legislación, sí adecuó de forma previa su normativa nacional incorporando un catálogo de delitos informáticos tales como; el acceso ilícito a bancos de datos personales además de su distribución; la vulneración de datos o sistemas informáticos y la interceptación de comunicaciones, entre otros. Asimismo, amplió la definición de ciertos conceptos.

En materia procesal fue más complejo al tratarse de un Estado federal y por esta razón cada provincia cuenta con su propia normativa procesal penal. Por lo tanto, no existe regulación general sobre medios informáticos. Son muy pocos los códigos procesales adelantados en el uso de pruebas electrónicas. Es en la provincia de Buenos Aires que el 2021 se aprobó y promulgó el protocolo sobre la integridad de la *Evidencia Digital* para la investigación para la prosecución penal en la comisión de los delitos informáticos.

Por otro lado, España es signataria del Convenio sobre Ciberdelincuencia 2001 pero fue en el año 2010 que fue promulgado. Las medidas de adecuación adoptadas se encuentran incorporadas plenamente en la legislación española en su derecho penal. Actualmente su sistema procesal penal, sustituyo la ley de Enjuiciamiento Criminal de 1882. Por lo que su normativa procesal penal, cuenta con un protocolo y uso de estándares informáticos para la obtención, análisis y de la evidencia digital.

En la revisión, Estados Unidos a pesar de no ser un miembro de la Unión Europea, sí es firmante y ha ratificado la Convención de Budapest de 2001 adaptando su legislación plenamente en la rama penal.

México no se ha adherido al Convenio porque existen grandes incompatibilidades para adecuar el Tratado con su Carta Magna, Código Penal y Código Procesal Penal. Sin embargo, este Estado es pionero en llamar *Delitos Informáticos* a las acciones antijuridicas cometidas por un medio informático y mediante el *Internet*. Asimismo, la legislación mexicana cuenta con un listado de delitos informáticos muy similares a los contenidos el Convenio. Sobre el derecho procesal penal México tiene normado un Protocolo, no solo sobre la Evidencia *Digital* sino también sobre la investigación en la persecución penal en las acciones antijuridicas cometidas por medio e intermedio de las Tecnologías de la Información y Comunicación.

En el caso boliviano, si bien se han tipificado los *Delitos Informáticos* en el Código Penal Boliviano, lo que evidencia que se encuentran dentro de su ordenamiento jurídico; no existe normativa procesal penal que aborde por lo menos una definición legal de *Evidencia Digital;* tampoco existen protocolos de uso generalizado por los expertos en ciencia forense que deba ser seguido para mantener la integridad de la mencionada prueba de manera que ésta pueda ser utilizada de idóneamente en una investigación penal sobre *Delitos Informáticos*

Conclusión al objetivo específico 2. “Analizar los Acuerdos y Tratados Internacionales relacionados con los delitos informáticos y la evidencia digital.”

Se han analizado los Acuerdos y Tratados Internacionales de la Unión Europea, Organización de los Estados Americanos y La Organización de las Naciones Unidas relacionados con los *Delitos Informáticos* y la *Evidencia Digital* y se concluye que es el Convenio Sobre Ciberdelincuencia de Budapest (Serie de Tratados Europeos No 185) de 2001 el instrumento internacional más completo. Se ha realizado una búsqueda de otras normativas internacionales sobre ciberdelitos y la evidencia digital, sin embargo, todas las que pudieron ser identificadas se remitían directamente a las disposiciones del Convenio de Budapest.

Si bien es cierto que este convenio es propio del Consejo Europeo, cabe enfatizar que se encuentra abierto a todos los países que deseen adherirse. De hecho, Estados Unidos de América, Argentina, Chile, Colombia, Japón y Marruecos, por ejemplo, ya lo han inclusive ratificado. El convenio está traducido a 4 idiomas de manera que pueda ser comprendido por una gran cantidad de Estados interesados en la lucha contra la ciberdelincuencia.

El Convenio de Budapest tiene dos pilares fundamentales y que abarcan ampliamente tanto en el *derecho penal sustantivo* que criminaliza ciertas conductas enlistadas en el mismo Convenio y el *derecho procesal penal* que dota a las autoridades en materia de procuración de justicia penal, las facultades y herramientas procedimentales necesarias para investigar la comisión de éstos delitos incluyendo la obligación de expandir las capacidades de inteligencia y vigilancia: tales como cateo e incautación de bienes, monitoreo de contenido en línea, retención y transferencia de datos o intervención de comunicaciones privadas.

Dentro del Derecho Penal Sustantivo se determina la existencia de 4 amplias categorías de delitos informáticos: 1. Delitos contra la confidencialidad, integridad y disponibilidad de los datos y sistemas informáticos; 2. Delitos Informáticos; 3. Delitos relacionados con el contenido y 4. Delitos relacionados con infracciones a la propiedad intelectual y derechos afines. Es la primera categoría, la de los delitos en contra la confidencialidad, integridad y disponibilidad de los datos y sistemas informáticos, la que es relevante para la presente investigación.

Los delitos informáticos de la primera categoría son los que deben ser regulados por los países miembros son: 1. El acceso ilícito, interceptación ilícita, ataques a la integridad de los datos, abuso de los dispositivos. 2. La falsificación y fraude informáticos. 3. Los delitos relacionados con la pornografía infantil y por ultimo los delitos relacionados con las infracciones de la propiedad intelectual y de derechos afines.

En el Derecho Procesal Penal las medidas procesales a tomarse en cuenta del Convenio son: las normas que corresponden tanto a las autoridades de investigación penal como a las autoridades judiciales. Estas normas son relativas al establecimiento de parámetros de

obtención y conservación de *Pruebas Electrónicas*, salvaguardando los derechos fundamentales de las personas.

El Convenio se ocupa de establecer distintos procedimientos para asegurar la integridad de la evidencia digital, de manera tal que pueda ser incorporada a un expediente investigativo. Para ello la información debe ser verificada y autentificada por los entes investigadores, comprobando que los datos no hayan sido alterados mediante la *Cadena de Custodia Digital* que asegura que la *Evidencia Digital* no ha sido modificada y que permanece integra ante la posibilidad de que otros lo hicieran.

El Convenio establece distintas herramientas, las cuales tienen por objetivo la obtención de los datos, estas medidas son:

1. La Conservación rápida de datos informáticos almacenados; 2. La conservación y revelación parcial rápida de los datos relativos al tráfico; 3. La orden de presentación; 4. El registro y confiscación de datos informáticos almacenados; 5. La obtención en tiempo real de datos relativos al tráfico; y 6. La interceptación de datos relativos al contenido.

El Estado Plurinacional de Bolivia no se ha adherido a este convenio constituyendo su único avance hacia esta temática la inclusión de los delitos de: Manipulación Informática y Alteración, Acceso y Uso Indebido de Datos Informáticos, que se encuentran tipificados los artículos 363 bis y 363 ter del Código Penal.

Conclusión al objetivo específico 3. “Exponer la necesidad de incluir el uso algorítmico en la búsqueda de la evidencia digital como prueba irrefutable para la averiguación de la verdad material en acciones antijurídicas en las Tecnologías de la información y comunicación”

El uso algorítmico para la obtención de la evidencia digital sí puede ser una manera de obtener una prueba irrefutable. La ciencia de la Informática Forense debe determinar los procedimientos idóneos para la averiguación de la verdad ante hechos antijurídicos relacionados con las TIC.

Si bien el algoritmo se constituye en la base fundamental de construcción, uso, goce y disposición de las Tecnologías de la Información y Comunicación, la creación y uso de éstos debe ser confiable debiendo cumplir con todos los requisitos de los estándares de calidad para su efectividad.

Para asegurar una investigación optima en la que primen el debido proceso y los derechos humanos en general los investigadores y autoridades judiciales deben ser capacitados en Derecho Informático e Informática Forense, la ciencia madre de las Tecnologías de la Información y Comunicación no con el objetivo de hacerlos técnicos similares a los peritos sino en el sentido de generar conciencia de la irrefutabilidad en potencia que tiene la evidencia digital si se sigue con un proceso óptimo para su obtención, hecho que es determinado por la calidad del algoritmo utilizado. Como consecuencia de esto se concluye que las instituciones relacionadas a la cadena de custodia de la evidencia digital deben estar dotadas de una infraestructura tecnológica capaz de tener dichos algoritmos actualizados y coincidentes con cambiantes desarrollos tecnológicos contemporáneos.

El análisis estadístico de la incidencia de los delitos informáticos en el país revela que:

Las denuncias por este tipo de delitos son más frecuentes en el Departamento de Santa Cruz con un 60% seguidas por las que se dan en el Departamento de La Paz con un 30% y El Departamento de Cochabamba con un 9%.

El tipo de delitos que se comenten en un mayor porcentaje son los de *Manipulación informática* en un 80% y el de *Alteración, acceso y uso indebido de datos informáticos* en un 23%.

El uso de la informática forense como el procedimiento de obtención de la evidencia digital en la región es:

1. Que la recolección de la evidencia digital responde al uso de algoritmos matemáticos.
2. Que el análisis de la evidencia digital debe responder al uso de algoritmos matemáticos.

3. Que la interpretación de la evidencia digital responde al uso de algoritmos matemáticos.
4. Que estos algoritmos cada día que pasa deben cumplir con más requisitos de calidad para su efectividad.

RECOMENDACIONES:

Habiéndose terminado el estudio propuesto, se tienen las siguientes recomendaciones:

Primera. El Estado boliviano debe adherirse al Convenio de Budapest de 2001 o por lo menos utilizar su contenido como base para la determinación de medidas a ser tomadas para optimizar el proceso de identificación de la verdad material en el caso de hechos antijurídicos relacionados con el uso de las TIC.

Segunda. Debe incrementarse un artículo de procedimiento como el Articulo 177 previsto en el Articulo 174 sobre la identificación y levantamiento de cadáver del Código Procesal Penal boliviano en el sentido de agregar específicamente los pasos fundamentales a seguirse para garantizar la conservación de la evidencia digital ante delitos cometidos con el uso de las TIC.

Tercera. El proceso de recolección de la evidencia digital debe ser realizado por medio del uso de algoritmos matemáticos reconocidos a nivel internacional como idóneos para dicho fin, de manera que se tenga a disposición de las autoridades siempre la herramienta idónea para la identificación de la evidencia.

Cuarta. Se debe trabajar con las autoridades relacionadas con el proceso penal para concientizarlas sobre la posibilidad de identificar de manera irrefutable la existencia de un delito por medio del correcto uso de los algoritmos matemáticos, de esta manera se podrá comprender que, para la averiguación de la verdad material, tener datos procesados por un algoritmo matemático idóneo es tan importante como tener una huella digital, un cadáver, o puerta abierta por la fuerza.

Quinta. El protocolo que sea adoptado por el Estado para el procesamiento de la evidencia digital debe contener mínimamente lo siguiente:

I.

1.1. Recursos Humanos

Dentro del proceso de investigación en la recolección, análisis e interpretación de la *Evidencia Digital*, se deberá designar un abogado penalista experto en derecho informático, un informático forense, un ingeniero de sistemas y/o ingeniero en telecomunicaciones.

1.2. Dispositivo De Almacenaje

A nivel institucional dentro del proceso de investigación en la recolección, análisis e interpretación de la *Evidencia Digital*, se deberá dotar de medios electrónicos y cuentas digitales en la nube, con número de serie y contraseñas firmas físicas y electrónicas por la máxima autoridad institucional.

En estos medios electrónicos, deberá almacenarse toda la *Evidencia Digital*, en base a la integridad, confiabilidad y disponibilidad de la misma en todas las instancias investigativas.

1.3. Bitácora

Dentro del proceso de investigación en la recolección, análisis e interpretación de la *Evidencia Digital*, los encargados y responsables deberán llenar y consignar todas las actividades realizadas, tomándose en cuenta todas y cada una de las actividades desarrolladas sin omitir detalle alguno.

II

2.1. Evidencia Digital

Dentro del proceso de investigación en la recolección, análisis e interpretación de la *Evidencia Digital*, los encargados y responsables deberán acreditar la extracción y recolección de la *Evidencia Digital*, mediante la captura íntegra de la misma, utilizando mecanismos de no intromisión que alteren a la misma.

2.2. Integridad de la Evidencia Digital

Dentro del proceso de investigación del proceso de investigación en la recolección, análisis e interpretación de la *Evidencia Digital*, los encargados responsables deberán garantizar la integridad mediante los principios de la informática forense: identificar, obtener y preservar la evidencia digital para demostrar que la misma no ha sido alterada. Así mismo rastrear, enjuiciar, interpretar, documentar y presentar las evidencias digitales para su investigación

La integridad de la *Evidencia Digital* debe responder al uso algorítmico conjunto de elementos encadenados y que convierte la *Evidencia Digital* en valores finitos de longitud fija expresados en vectores alfanuméricos.

III

3.1. Análisis Forense

Para los casos específicos, donde se requiere recuperar o editar archivos digitales dentro de dispositivos electrónicos que han sido dañados, los encargados del proceso de investigación en la recolección, análisis e interpretación de la *Evidencia Digital*, podrán utilizar Software Forense que deberá estar certificado en su explotación, mediante manuales de funciones y procedimientos a fin de garantizar el medio operativo del Software Forense validos de la explotación de los recursos informáticos forenses para cuantificar y calificar el daño producido en contra de los dominios tecnológicos.

3.2. Software Forense Libre

Dentro del proceso de investigación, se podrá utilizar herramientas de *Software Libre*, cumpliéndose los siguientes requisitos:

a) La herramienta deberá pasar por un proceso de control de calidad que garantice la no alterabilidad de la Evidencia Digital.

b) Los encargados del proceso de investigación en la recolección, análisis e interpretación de la Evidencia Digital deberán realizar procesos de auditoria para certificar la funcionalidad de los algoritmos del Software Libre.
c) Los cambios o transformaciones realizadas al Software Libre deberán estar destinados exclusivamente al objeto forense, siendo limitativa y excluyente la adecuación del Software para fines ilícitos.
d) Todas las herramientas forenses de Software Libre deberán estar debidamente documentadas para demostrar en instancias judiciales el uso procedimental de la misma.

3.3. Software Forense con licencia

En caso de utilizarse herramientas forenses con licencia, éstas deberán cumplir los siguientes requisitos:

a) La herramienta deberá pasar por un proceso de control de calidad que garantice la no alterabilidad de la Evidencia Digital
b) Las licencias deben estar vigentes.
c) No podrán realizarse cambios o transformaciones al *Software Licenciado*.

IV

4.1. Informática Forense

Será el medio procedimental, mediante la construcción de *algoritmos abiertos* y auditables para la captura, recolección, conservación, resguardo, almacenamiento, análisis e Interpretación de la *Evidencia Digital*.

4.2. Algoritmo Matemático

Sera el que se emplee, para expresar las relaciones, proposiciones sustantivas de hechos, variables, parámetros, entidades y relaciones entre variables de las

operaciones, que permitan establecer los comportamientos de sistemas complejos dentro de las Tecnologías de la Información y Comunicación a fin de observar en la realidad.

Estos algoritmos estarán construidos, cumpliéndose los siguientes requisitos:

a) Algoritmos cualitativos o conceptuales, estos pueden usar figuras, gráficos o descripciones causales, en general se contentan con predecir si el estado del sistema irá en determinada dirección o si aumentará o disminuirá alguna magnitud, sin importar exactamente la magnitud concreta de la mayoría de los aspectos.
b) Algoritmos cuantitativos o numéricos, usan números para representar aspectos del sistema modelizado, y generalmente incluyen fórmulas matemáticas más o menos complejos que relacionan los valores numéricos. El cálculo con los mismos permite representar el proceso físico o los cambios cuantitativos del sistema modelado.
c) Algoritmo de simulación o descriptivo, de situaciones medibles de manera precisa o aleatoria, por ejemplo, con aspectos de programación lineal cuando es de manera precisa, y probabilística o heurística cuando es aleatorio. Este tipo de algoritmos pretende predecir qué sucede en una situación concreta dada.
d) Algoritmos de optimización. Para determinar el punto exacto para resolver alguna problemática administrativa, de producción, o cualquier otra situación. Cuando la optimización es entera o no lineal, combinada, se refiere a algoritmos matemáticos poco predecibles, pero que pueden acoplarse a alguna alternativa existente y aproximada en su cuantificación. Este tipo de algoritmos requiere comparar diversas condiciones, casos o posibles valores de un parámetro y ver cuál de ellos resulta óptimo según el criterio elegido.
e) Algoritmo de control. Para saber con precisión como está algo en una organización, investigación, área de operación, etc. Este algoritmo

pretende ayudar a decidir qué nuevas medidas, variables o qué parámetros deben ajustarse para lograr un resultado o estado concreto del sistema modelado.

Estos algoritmos matemáticos deberán ser clasificados en conformidad a su funcionalidad en las Tecnologías de la Información y Comunicación , de acuerdo a la siguiente tabla:

a.	Cálculos astronómicos
b.	Simulaciones de tráfico
c.	Cálculo componentes de sistemas
d.	Diseño ingenieril
e.	Control automático
f.	Análisis microeconómicos
g.	Teoría de juegos

Tabla: Elaboración Propia

4.3. Fases para la construcción de un algoritmo matemático

Fase1. Identificación de un problema o situación compleja que necesita ser simulada, optimizada o controlada.

Fase2. Elección del tipo de algoritmo, esto requiere precisar qué tipo de respuesta pretende obtenerse, cuáles son los datos de entrada o factores relevantes, y para qué pretende usarse el algoritmo. Esta elección debe ser suficientemente simple como para permitir un tratamiento matemático asequible con los recursos disponibles. Esta fase requiere además identificar el mayor número de datos fidedignos, rotular y clasificar las incógnitas (variables independientes y dependientes).

Fase3. Formalización del algoritmo en la que se detallará la forma que tienen los datos de entrada, el tipo de herramienta matemática que se usará.

En esta fase, se incluye la confección de algoritmos, ensamblaje de archivos informáticos.

Fase4. Comparación de resultados, si los resultados no son los esperados, es proceso deberá reiniciarse desde la fase 1

4.4.- Reconstrucción de los Hechos

Concluido y compilado el algoritmo, éste deberá ser aplicado en el proceso de reconstrucción de los hechos; para tal efecto, deberá ser acorde a las actividades detalladas en la bitácora de investigación.

V.

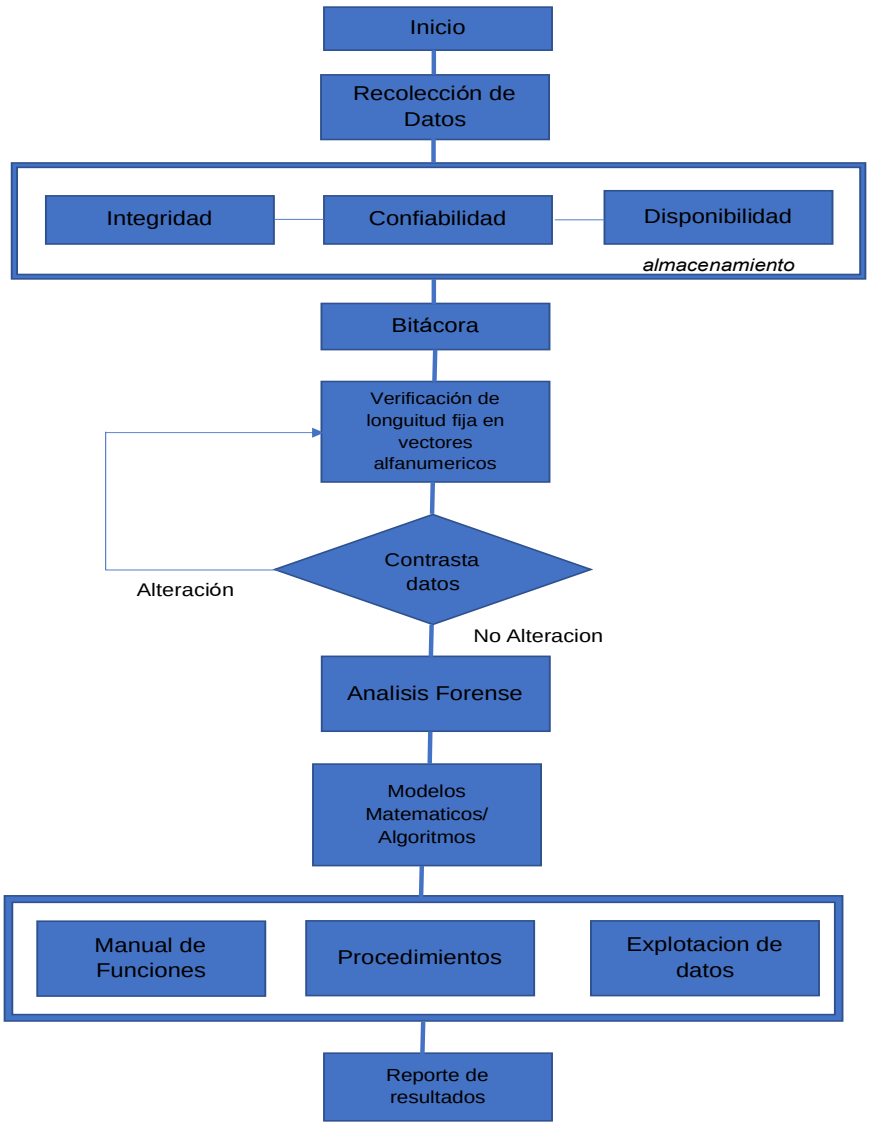
5.- Informes

Los responsables y encargados del proceso de investigación en la recolección, análisis e interpretación de la Evidencia Digital deberán elaborar dos tipos de informes:

1. *Informe Ejecutivo*. En el que se consigna un detalle ejecutivo de las actividades realizadas.

2. *Informe Técnico*. En el que se consiga un detalle pormenorizado de todas las actividades realizadas y acompañadas de todos los elementos probatorios lógicos y físicos.

Diagrama de flujo del Protocolo para la Cadena de Custodia Digita



Flujograma: Construcción Propia

Bibliografía

Gimeno. (2010).

ATT. (26 de 01 de 2018). *https/att.gob.bo*. (Nota de Prensa) Recuperado el 2018, de Autoridad de Regulizacion y Fiscalizacion de Telecomunicaciones y Transporte: https://www.att.gob.bo/content/el-acceso-internet-en-bolivia-el-2017-alcanzó-8817749-de-conexiones-fijas-y-móviles

Acurio Del Pino, S. (2006). *Delitos Informáticos.* PUCE.

Kelsen, H. (1982). *Teoría pura del Derecho.* Argentina: EUDEBA.

Kelsen, H. (1993). *Teoría pura del Derecho.* México: Porrúa.

Morrish, R. (1955). *The Police and Crime-Detection Today.* Oxford.

Moscoso, J. (2008). *Introducción al Derecho.* La Paz, Bolivia: Jueventud.

Koria, R. (2007). *La metodología de la Investigación desde la práctica didáctica.*

Zegarra, V. J. (2002). *Formas de Elaborar; Tesis, Tesinas y Proyectos de Grado.*

EIIDI. (2012). *Equipo de Investigacion de Incidentes y Delitos Informaticos*. Obtenido de EIIDI: http://www.EIIDI.com

Acurio Del Pino, S. (2014). *Manual de manejo de evidencias digitales y entornos informaticos.* Recuperado el 2018, de oas.org: https://www.oas.org/juridico/english/cyb_pan_manual.pdf

Meza-Lopehandia, M. (2014). *Los delitos ciberneticos en la legislacion estadounidense.* Obtenido de BCN Biblioteca Del Congreso Nacional de Chile: https://obtienearchivo.bcn.cl/obtienearchivo?id=repositorio/10221/20864/5/FINAL%20_%20Informe%20_%20Cibercrimen%20en%20EEUU_v5.pdf

Mayer Lux, L. (2017). EL BIEN JURÍDICO PROTEGIDO EN LOS DELITOS INFORMÁTICOS. *Revista Chilena de Derecho, 44*(1), 0716-0747.

Meza-Lopehandía, M. (2014). *Los Delitos Informaticos en la Legislacion estadounidense.* Santiago: Biblioteca del Congreso Nacional de Chile.

Gercke, M. (2018 de 2007). *Oficina de las Naciones Unidas Contra la Droga y el Delito.* Obtenido de unodc.com: https://www.unodc.org/documents/organized-crime/13-83700_Ebook.pdf

Lecours, A. (2007). *Despacho de Abogados*. (A. Lecours, Productor) Obtenido de ponce.inter.edu: https://ponce.inter.edu/cai/bv/LEY-PATRIOTA-DE-LOS-EE-UU-USA-PATRIOT-ACT.pdf

Yañez, A. (2020). *Scribd*. Obtenido de https://es.scribd.com/document/262118241/Manipulacion-de-La-Evidencia-Digital

BOE-A-2018-16673. (6 de Diciembre de 2018). *Agencia Estatal Boletin Oficial del Estado.* Recuperado el 2018, de https://www.boe.es/eli/es/lo/2018/12/05/3: https://www.boe.es/buscar/doc.php?id=BOE-A-2018-16673

Slideshare. (29 de julio de 2013). Obtenido de https://es.slideshare.net/grimis/seguridad-delitos?from_action=save

OEDI. (2021). *Observatorio Español de Delitos Informaticos*. Recuperado el 2022, de https://oedi.es/estadisticas/

Codigo Penal de Sinaloa Mx. (1992).

SEGOB. (2016). *Protocolo de actuacion para la obtencion y tratamiento de los recursos iformaticos y/o evidencias digitales.* Obtenido de SEGOB Secretaria de la Gobernacion: https://www.dof.gob.mx/nota_detalle.php?codigo=5441707&fecha=17/06/2016#gsc.tab=0

Ciberdelito. (2022). *argentina.gob.com.* Recuperado el 2022, de https://www.argentina.gob.ar/justicia/convosenlaweb/situaciones/que-es-el-ciberdelito

Temperi, M. (2013). *El Derecho Informatico.* Recuperado el 2021, de http://elderechoinformatico.com/publicaciones/mtemperini/CONAIISI_Temperini_Camera_Ready.pdf:

http://elderechoinformatico.com/publicaciones/mtemperini/CONAIISI_Temperini_Camera_Ready.pdf

AFI. (2020). *Protocolo para la estadarizacion del procedimientos de obtencion de evidencia digital.* Obtenido de AFI: https://www.argentina.gob.ar/inteligencia

Pérez Pereira, M. (s.f.). *Electrónica de Derecho Informático.* Obtenido de http://derecho.org/redi

Nuñez Ponce, J. (1996). *Derecho Informático: Concepto y diferencias con la informática jurídica Autonomía y metodología del Derecho Informático.* Marsol.

Martin Nessi, A. (2017). *mpfn.gob.pe*. Obtenido de https://www.mpfn.gob.pe/Docs/0/files/manual_evidencia_digital.pdf

Acurio Del Pino, S. (2010). *OAS*. (S. A. Pino, Productor) Obtenido de oas.org: https://www.oas.org/juridico/english/cyb_pan_manual.pdf

Diccionario Panhispánico, D. (2005). *El término "evidencia" es la 'categoría absoluta que no admite dudas' o la 'certeza clara y manifiesta de la verdad o realidad de algo.*

Molina Ochoa,C, Beltran Bermudez Caterin, Contreras Martinez Olga. (2020). La Prueba Electronica y Digital. Aclaracion de las diferencias juridicas en Colombia. *Proyectos de Investigacion Migracion y Trata de personas*, 11-37.

Tecnologia. (28 de octubre de 2020). *Independente Español*. Recuperado el 11 de abril de 2022, de independentespanol.com: https://www.independentespanol.com/tecnologia/seccion-230-regla-internet-twitter-facebook-google-b1401498.html

SeguInfo. (2001). Obtenido de https://www.segu-info.com.ar/delitos/china

LaRed. (10 de agosto de 2021). Recuperado el 2021, de https://www.lared.am/mundo/china-condena-pena-muerte-un-canadiense-narcotrafico-n853258

Barreto, A. (2000). Codigo Penal Aleman. *Codigo Penal Aleman (Traduccion)*.

Ciberseguridad. (2019). Obtenido de https://ciberseguridad.com/normativa/europea/alemania/

Mosquera G, J. A. (2004). *Evidencia Digital en el contexto Internacional, la necesidad de un estandar.* Colombia: Universidad De Los Andes.

Manzanera, L. (2019). Observacion de las Buenas Prácticas en el Reino Unido. *revista digital de los CEP* (21), 15 - 17.

Biblioteca Del Congreso Nacional de Chile, B. L. (7 de junio de 1993). *Ley 19223.* Recuperado el 2021, de http://bcn.cl/: http://www.bcn.cl/2by7s

Biblioteca del Congreso Nacional de Chile, B. (28 de febrero de 2020 Ultima Modificación). *Ley 21214.* Recuperado el 2021, de http://www.bcn.cl/: http://www.bcn.cl/2er4q

Informáticos, P. q. (13 de marzo de 2022). *Senado de la República de Chile.* Recuperado el 2022, de República de Chile, Senado: https://www.senado.cl/budapest

García, P. I. (2002). Derecho Nuevas Tecnologías.

Peñaranda Quintero, H. R. (s.f.).

Peñaranda Quitero, H. R. (2007). *IUSCUBERNÉTICA: Interrelación entre el Derecho e Informática.* Maracaibo, Venezuela.

Witker, J. (1999). *Metodología de la investigación jurídica.* Mc.Graw- Hill.

Ibañez, R. M. (2003). *Metodología de la investigación.* Artes Gráficas Sagitario S.R.L.

Mostajo, M. (2005). *Seminario Taller de Grado.*

Leavitt, H. J., & Whisler, T. L. (1958). *Management in the 1980s.*

Butler, J. G. (2012). *A History of Information Technology and Systems.* Arizona: University of Arizona.

Roig, F. (s.f.). *Tecnología de la información Conceptos básicos.*

Hilbert, M., & López, P. (2011). *The World's Technological Capacity to Store, Communicate, and Compute Information.* Science 332 (6025).

Rincon, J. (2005). *Concepto de Sistemas y Teoría General de Sistemas.*

Gomez, V. Á. (2007). *Enciclopedia de la Seguridad Informática.*

Vicens, E., & Guarich, J. (1997). *Métodos Cuantitativos Volumen I.* Valencia: Servicio de Publicaciones.

Wymore, A. W. (1972). *Mathematical Theory of Sistems Engineering: The Elements.* New York: Palisade.

Pressman, R. S. (2005). *Ingeniería de Software: Un Enfoque Práctico* (Sexta Edición ed.). México: McGraw Hill.

Anónimo. (s.f.). Planning Extreme Programming. Addison-Wesley.

Muñoz Conde, F., & García Arán, M. (2004). *Derecho Penal. Parte General* (Sexta Edición ed.). Valencia: Tirant lo Blanch.

Tellez Valdez, J. (s.f.). *Derecho Informático.* México: Mc. Graw - Hill .

Devis Echandía, H. (2005). *Teoría General de la Prueba.* Bogotá, Colombia: Temis S.A.

Devis Echandía, H. (s.f.). *Breve Historia de las Pruebas Judiciales-Teoría General de la Prueba Judicial.*

Devis Echandía, H. «. (s.f.).

Senso, J. A., & Rosa Piñero, A. d. (2003). *El concepto de metadato. Algo más que descripción de recursos electrónicos* (Vol. 32). Ciência da Informação.

Bray, T. (9 de junio de 1998). RDF and Metadata.

Sheldon, T. (2001). Metadata. Linktionary.

Steinacker, A., Ghavam, A., & Steinmetz, R. (2001). Metadata Standards for Web-Based Resources. IEEE MultiMedia.

W3C, R. S. (2002). Metadata Activity Statement.

Bultermann, D. C. (2004). Is It Time for a Moratorium on Metadata. *IEEE Multimedia, 11(4), IEEE Computer Society Press:10-17.* USA: Los Alamitos.

Durrell, W. R. (1985). Data Administration. A Practical Guide to Data Administration. McGraw-Hill.

Wiener, N. (1980). Cibernética y sociedad. 20. Fe E.

Reyes Echandía, A. (1981). *La Tipicidad.* Colombia: Universidad de Externado de Colombia.

https://www.incibe-cert.es/blog/rfc3227. (s.f.).

García, P. I. (14 de febrero de 2002). Derecho Nuevas Tecnologías.

Reyes Echandía, A. (1981). *La Tipicidad.* Colombia: Universidad de Externado de Colombia.

Gimeno, V. A. (2010). *LA INFLUENCIA DE LAS NUEVAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES Y SU REPERCUSIÓN EN LAS ESTRATEGIAS EMPRESARIALES: LA BANCA ONLINE Y SU APLICACIÓN EN LAS COOPERATIVAS DE CRÉDITO.* Valencia , España.

Pinochet Olave, Ruperto Andres, Arancibia Obrador, Maria Jose. (2011). CARACTERIZACIÓN DEL NEGOCIO JURÍDICO ELECTRÓNICO A LA LUZ DE LA TEORÍA GENERAL DEL ACTO JURÍDICO . *revista De DerechO y ciencias Penales no 17 (23-41), 2011, Universidad San Sebastián (Chile)*(17), 23-41.

Sacoto-Regalado, S. P., & Cabrera-Duffaut, A. (2020). Aplicación de la técnica de Focus Group para la validación del despliegue del correo electrónico utilizando una solución Cloud Computing. *Dominio de las Ciencias,, 6*(4), 962-976.

https://www.segu-info.com.ar/. (24 de Enero de 2001). Recuperado el 2021, de https://www.segu-info.com.ar/delitos/china

https://es.slideshare.net/mmazonf/. (14 de marzo de 2019). Recuperado el 2019, de https://es.slideshare.net/mmazonf/informatica-forense-136353407

Barreto, A. (s.f.). Codigo Aleman TRaducido al Español. *Codigo Penal*.

Gimeno. (Marzo de 2010). *Revista electrónica Ciencia e innovación tecnológica en el deporte* (11).

Pinochet,R, Arancibia, M. (2011). Caracterización del negocio jurídico electrónico a la luz de la teoría. . *Derecho y Ciencias Penales*(17), 23-41.

CPE. (7 de Febrero de 2009). *Constitución Política del Estado*. Bolivia.

Moscoso, J. (2008). *Introducción al derecho.* La Paz. Bolivia: Jueventud.

Policia Nacional Española. (s.f.).

Barrios A., V. (Julio de 2018). *BCN*. (B. d. Parlamentario, Productor) Recuperado el 2022, de https://obtienearchivo.bcn.cl/obtienearchivo?id=repositorio/10221/26882/1/Convenio_de_Budapest_y_Ciberdelincuencia_en_Chile.pdf

UNODC. (2021). *unodc.org*. Obtenido de https://www.unodc.org/documents/ropan/2021/PANZ41/Aspectos_basicos_de_la_investigacion_que_involucra_prueba_digital.pdf

Acurio Del Pino, S. (2014). *oas.org*. Recuperado el 2019, de https://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

UNODC. (2 de febrero de 2015). *unodc.org*. Recuperado el 2021, de https://www.unodc.org/documents/congress/Documentation/A-CONF.222-12_Workshop3/ACONF222_12_s_V1500666.pdf

Interpol. (2022). *interpol.int/es/* . Recuperado el 2022, de https://www.interpol.int/es/Como-trabajamos/Innovacion/Analisis-forense-digital

Borzi, F. (2018). *pensamientopenal.com.ar* . Recuperado el 2022, de https://www.pensamientopenal.com.ar/system/files/2018/09/doctrina46963.pdf

Christy, D. (junio de 1980). Computer Crime a Growing Menace. *Military Police*. Recuperado el 2022, de books: https://books.google.com.bo/books?id=Sv45AQAAMAAJ&pg=RA6-PA26&lpg=RA6-

PA26&dq=El+FCIC+(Federal+Computers+Investigation+Committee)&source=bl&ots=MhMCStBWeA&sig=ACfU3U1tQirXBUaBp72x3MCaNm6zsGl3Ew&hl=es&sa=X&ved=2ahUKEwjp5r2GqYb3AhXjrpUCHZ0bAtAQ6AF6BAgREAM#v

Garcia Collantes, A. (15 de Mayo de 2018). *Colegio de Criminologos de la Comunidad de Madrid*. (A. G. Collantes, Productor, & Colegio de Criminologos de la Comunidad de Madrid) Recuperado el 2018, de https://colegiocriminologosmadrid.es/el-principio-de-intercambio-de-locard/

Godoy F, T. (2019). Los subsistemas jurídicos británicos (derecho consuetudinario inglés o common law) y el sistema judicial español (civil law). *Derecho Mexicano*, 52-154, 513-538.

Romero C, Martha; Choez Ch, Miguel; Alava M, Crhistian; Romero C, Vicente; Castillo M, Miriam; Murillo Q, Leonardo; Delgado L, Holger. (Septtiembre de 2020). *3Ciencias*. Recuperado el 2021, de 3ciencias.com: https://www.3ciencias.com/wp-content/uploads/2020/09/LA-INFORMÁTICA-FORENSE-DESDE-UN-ENFOQUE-PRÁCTICO.pdf

Info-Lab. (2016). Recuperado el 2022, de Guia Integral de empleo de la Informatica Forense en el Proceso Penal: http://redi.ufasta.edu.ar:8082/jspui/bitstream/123456789/1592/2/PAIF.pdf

Conicet. (2021). *Protocolo De Actuacion Para la Investigacion Cientifica en el Lugar del Hecho.* Recuperado el 2022, de Conicet.gov.ar/: https://www.conicet.gov.ar/wp-content/uploads/anexo_6486329_1.pdf

Niño, D. Y. (1 de abril de 2022). Los Datos Personales y sus riesgos juridicos a partir de klka transformacion digital en el Comercio Electronico. *Revista CES Derecho, 13*(1), 72.

Proyecto Hola, Principado de Asturias, Formacion Academica. (2014). *Proyecto Hola.* Recuperado el 2022, de https://www.uv.mx/personal/rcordoba/files/2014/11/Correo_electronico.pdf

Tellez Aguilera, A. (2009). *Criminología.* Madrid , España: Edisofer.

González M, S. (2006). COMERCIO ELECTRÓNICO Y LEY APLICABLE AL NEGOCIO JURÍDICO ELECTRÓNICO. *Revista Boliviana de Derecho. Disponible en: https://www.redalyc.org/articulo.oa*(1), 141-155.

Condomi, A. (www.saij.gob.ar Id SAIJ: DACF200179 de 2020). Qué queda de la "norma fundante básica presupuesta" de Kelsen? *Qué queda de la "norma fundante básica presupuesta" de Kelsen?* Buenos Aires, República de Argentina.

Franciéllen de Barros; Barbara Kuhnen; Mônica da Costa Serra; Clemente Maia da Silva Fernandes. (2020). Ciencia Forense: Principio éticos y sesgos. *Revista Bioetica, 29*(1).

IACIS. (2022). Recuperado el 2022, de https://www.iacis.com

Organización de los Estados Americanos. (23 de 11 de 2001). *Convenio Sobre Ciberdelincuencia.* Recuperado el 2021, de www.oas.org: https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

Fucito, F. (1989). Concepción Sociológica del Derecho. *Cuadernos de Investigaciones Nro. 10*(10), 1-45. Obtenido de derecho.uba.ar: http://www.derecho.uba.ar/investigacion/Cuadernos_de_Investigacion10.pdf

QuestionPro. (13 de julio de 2022). *questionpro*. Obtenido de www-questionpro.com: https://www.questionpro.com/blog/es/entrevista-estucturada-y-no-estructurada/

Mayer, Laura ; Calderon, Guillermo. (30 de 06 de 2020). El Delito de Fraude Informatico. *Revista Chilena de Derecho y Tecnologia, 9*(1), 157.

Acurio Del Pino, S. (2016). *Delitos Informaticos.* Recuperado el 2018, de oas.org: https://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

Villalva, C., Jasso, J., & Olmos, M. (2004). *La Prueba Electrónica.* Bogotá, Colombia: Temis.

Taruffo, Michele; Vazquez, Ma.delCarmen; Ferrer Jordi. (2018). Teoria de la Prueba. *Trubunal Constitucional Plurinacional Academia Plurinacional de Estudios constitucionales, Edicion Especial*, 25.

Cruz, E. (2014). Modelo para el analisis y gestion de riesgos en fases carentesmde tecnicas herramientas Caso Tretamiento de la Evidencia Digital en el entorno del software libre utilizando procesos unificados. *PG1*.

Fondo de Apoyo Periodístico “La Paz y Tarija a través de nuevas miradas”, q. i. (14 de 09 de 2020). *Comunidad de Derechos Humanos*. Obtenido de https://comunidad.org.bo/index.php/noticia/detalle/cod_noticia/9602: https://comunidad.org.bo/index.php/noticia/detalle/cod_noticia/9602

Division Forensic Computer. (2022). *Division Forensic Computer.* Obtenido de https://www.delitosinformaticos.info/: https://www.delitosinformaticos.info/delitos_informaticos/legislacion

Codigo Penal de la Nacion Argentina. (2019). *https://www.argentina.gob.ar/sites/default/files/proyecto_de_nuevo_codigo_penal_de_la_nacion.pdf.*

Orta, R. (2023). *Criminalistica.Net Portal de Criminalistica y Ciencias Forenses.* Obtenido de Criminalistica.net/crimen-y-ciencia-forense/: https://criminalistica.net/crimen-y-ciencia-forense/

UNE Normativa Española. (2022). Obtenido de UNE Normativa Española: https://www.une.org/encuentra-tu-norma/busca-tu-norma/norma?c=N0051411

López, M. (2007). *Análisis Forense Digital* (Segunda Edición ed.). CriptoRed.

Senado Argentino. (24 de Junio de 2008). Codigo Penal Modificacion de la Ley 26388. Buenos Aires, Buenos Aires, Argentina. Obtenido de https://www.oas.org/juridico/PDFs/arg_ley26388.pdf: https://www.oas.org/juridico/PDFs/arg_ley26388.pdf

José Alejandro Mosquera González - Andrés Felipe Certain Jaramillo - Jeimy J. Cano. (2005). Evidencia digital:. *Didalnet*.

Ramos Álvarez, Benjamin Ribagorda Garnacho, Arturo. (2004). *Avances en Criptografia y seguridad de la informacion.* Malaga - España: Diaz de Santos.

Fundacion Construir. (2019). *https://www.fundacionconstruir.org*. Obtenido de Primer Diagnostico sobre Ciberdelincuencia en Bolivia: https://www.fundacionconstruir.org/wp-content/uploads/2021/02/Bolet%C3%ADn-Ciberdelincuencia.pdf

CONICET. (2021). *conicet.gov.ar/*. Recuperado el 2022, de Ministerio De Seguridad-Argentina: https://www.conicet.gov.ar/wp-content/uploads/anexo_6486329_1.pdf

Mandamiento Ortiz, Arturo; Ruiz Aponte, Domingo. (2017). *El método deductivo-inferencial y su eficacia en el aprendizaje de la matemática de los estudiantes del primer año de secundaria de la I.E. "José María Arguedas" San Roque – Surco – 2014.* Peru.

LISA Instituto. (2023). Cadena de Custodia Digital. España.

Manual de Actuaciones Investigativas de Fiscales, Policías y Peritos. (22 de Febrero de 2007). *RESOLUCIÓN CONJUNTA DE LA FISCALIA GENERAL DE LA REPUBLICA Y COMANDO GENERAL DE LA POLICIA NACIONAL No 001/2007* . Cochabamba, Bolivia. Obtenido de https://comunidad.org.bo/assets/archivos/herramienta/ae3e9ee5d69d381609d620ce509340ff.pdf: https://comunidad.org.bo/assets/archivos/herramienta/

Ministerio Publico. (2012). *https://migracion.gob.bo/sites/default/files/2021-06/N°%20260%20-%20LEY%20ÓRGANICA%20DEL%20MINISTERIO%20PÚBLICO%20-%2011-07-2012.pdf.* Obtenido de https://migracion.gob.bo/sites/default/files/2021-06/N°%20260%20-%20LEY%20ÓRGANICA%20DEL%20MINISTERIO%20PÚBLICO%20-%2011-07-2012.pdf

RAE. (2022). *Real Academia Española*. Obtenido de https://dle.rae.es/: https://dle.rae.es/algoritmo

Takeyas, B. L. (2019). *Tecnologico Nacional de Mexico*. Obtenido de Conceptos Algoritmicos: http://www.itnuevolaredo.edu.mx/takeyas/libroisc/03.-ConceptosAlgoritmos.pdf

Francachs Castro, B. (2021). Modelos Para la Obtencion de Evidencias Digitales en la Nube. *Revista de Posgrado de Informatiza de UMSA*.

(s.f.).

ANEXOS

ANEXO 1

Algoritmo Matemático de simulación para la obtención de evidencias digitales para el delito 363 Bis.- Manipulación Informática.

CLEMENCIA ELENA CARRANZA BRAVO

Modelo matematico como aproximacion a la identificacion de delitos informaticos

CASO: Detección de fraudes en transacciones financieras

Uso de una billetera móvil podemos identificar de todas las transacciones que se realizan cuales corresponden a fraudes.

In [35]:
```
import pandas as pd
import numpy as np
import math

%matplotlib inline
import matplotlib.pyplot as plt
import seaborn as sns

from sklearn.model_selection import train_test_split
from sklearn.ensemble import RandomForestClassifier

from sklearn.metrics import accuracy_score, confusion_matrix, precision_score, recall_score,roc_auc_score, roc_curve, f1_score
```

In [36]:
```
pwd
```

Out[36]:
```
'/Users/clemenciac'
```

PASO 1: CARGADO DE DATOS

In [38]:
```
df=pd.read_csv(r'/Users/clemenciac/desktop/fraude_tesis.csv')

df.head(22)
```

PASO 1: CARGADO DE DATOS

In [38]:
df=pd.read_csv(r'/Users/clemenciac/desktop/fraude_tesis.csv')

df.head(22)

Out[38]:

	Tiempo	Tipo	Monto	Nombre_cliente	Saldo_Inicial_antes_transaccion	Nuevo_saldo_cliente	Nombre_destinatario	Balance_anterior_destinatario	Nuevo_balance_destinatario	Es_fraud
0	1	PAGO	9839.64	C1231006815	170136.00	160296.36	M1979787155	0.00	0.00	
1	1	PAGO	1864.28	C1666544295	21249.00	19384.72	M2044282225	0.00	0.00	
2	1	TRANSFERENCIA	181.00	C1305486145	181.00	0.00	C553264065	0.00	0.00	
3	1	RETIRO_DINERO	181.00	C840083671	181.00	0.00	C38997010	21182.00	0.00	
4	1	PAGO	11668.14	C2048537720	41554.00	29885.86	M1230701703	0.00	0.00	
5	1	PAGO	7817.71	C90045638	53860.00	46042.29	M573487274	0.00	0.00	
6	1	PAGO	7107.77	C154988899	183195.00	176087.23	M408069119	0.00	0.00	
7	1	PAGO	7861.64	C1912850431	176087.23	168225.59	M633326333	0.00	0.00	
8	1	PAGO	4024.36	C1265012928	2671.00	0.00	M1176932104	0.00	0.00	
9	1	DEBITO	5337.77	C712410124	41720.00	36382.23	C195600860	41898.00	40348.79	
10	1	DEBITO	9644.94	C1900366749	4465.00	0.00	C997608398	10845.00	157982.12	
11	1	PAGO	3099.97	C249177573	20771.00	17671.03	M2096539129	0.00	0.00	
12	1	PAGO	2560.74	C1648232591	5070.00	2509.26	M972865270	0.00	0.00	
13	1	PAGO	11633.76	C1716932897	10127.00	0.00	M801569151	0.00	0.00	
14	1	PAGO	4098.78	C1026483832	503264.00	499165.22	M1635378213	0.00	0.00	
15	1	RETIRO_DINERO	229133.94	C905080434	15325.00	0.00	C476402209	5083.00	51513.44	
16	1	PAGO	1563.82	C761750706	450.00	0.00	M1731217984	0.00	0.00	
17	1	PAGO	1157.86	C1237762639	21156.00	19998.14	M1877062907	0.00	0.00	
18	1	PAGO	671.64	C2033524545	15123.00	14451.36	M473053293	0.00	0.00	
19	1	TRANSFERENCIA	215310.30	C1670993182	705.00	0.00	C1100439041	22425.00	0.00	
20	1	PAGO	1373.43	C20804602	13854.00	12480.57	M1344519051	0.00	0.00	
21	1	DEPOSITAR_DINERO	143236.26	C1862994526	0.00	143236.26	C1688019098	608932.17	97263.78	

Se eliman columnas que no son parte del analisis puntual del modelo matemático como ser el nombre del cliente y el nombre del destinatario

In [60]:
```
df1=df.drop(columns=['Nombre_cliente','Nombre_destinatario'])
df1.head(26)
```

Out[60]:

	Tiempo	Tipo	Monto	Saldo_Inicial_antes_transaccion	Nuevo_saldo_cliente	Balance_anterior_destinatario	Nuevo_balance_destinatario	Es_fraude	Intentos_ilegables
0	1	PAGO	9839.64	170136.00	160296.36	0.00	0.00	0	0
1	1	PAGO	1864.28	21249.00	19384.72	0.00	0.00	0	0
2	1	TRANSFERENCIA	181.00	181.00	0.00	0.00	0.00	1	0
3	1	RETIRO_DINERO	181.00	181.00	0.00	21182.00	0.00	1	0
4	1	PAGO	11668.14	41554.00	29885.86	0.00	0.00	0	0
5	1	PAGO	7817.71	53860.00	46042.29	0.00	0.00	0	0
6	1	PAGO	7107.77	183195.00	176087.23	0.00	0.00	0	0
7	1	PAGO	7861.64	176087.23	168225.59	0.00	0.00	0	0
8	1	PAGO	4024.36	2671.00	0.00	0.00	0.00	0	0
9	1	DEBITO	5337.77	41720.00	36382.23	41898.00	40348.79	0	0
10	1	DEBITO	9644.94	4465.00	0.00	10845.00	157982.12	0	0
11	1	PAGO	3099.97	20771.00	17671.03	0.00	0.00	0	0
12	1	PAGO	2560.74	5070.00	2509.26	0.00	0.00	0	0
13	1	PAGO	11633.76	10127.00	0.00	0.00	0.00	0	0
14	1	PAGO	4098.78	503264.00	499165.22	0.00	0.00	0	0
15	1	RETIRO_DINERO	229133.94	15325.00	0.00	5083.00	51513.44	0	0
16	1	PAGO	1563.82	450.00	0.00	0.00	0.00	0	0
17	1	PAGO	1157.86	21156.00	19998.14	0.00	0.00	0	0
18	1	PAGO	671.64	15123.00	14451.36	0.00	0.00	0	0
19	1	TRANSFERENCIA	215310.30	705.00	0.00	22425.00	0.00	0	0
20	1	PAGO	1373.43	13854.00	12480.57	0.00	0.00	0	0
21	1	DEPOSITAR_DINERO	143236.26	0.00	143236.26	608932.17	97263.78	0	0
22	1	DEPOSITAR_DINERO	228451.89	143236.26	371688.15	719678.38	1186556.81	0	0
23	1	DEPOSITAR_DINERO	35902.49	371688.15	407590.65	49003.30	0.00	0	0
24	1	DEPOSITAR_DINERO	232953.64	407590.65	640544.28	1172672.27	1517262.16	0	0
25	1	DEPOSITAR_DINERO	65912.95	640544.28	706457.23	104198.26	24044.18	0	0

PASO 2: Análisis de datos

In [55]:
```
df1.shape
```

Out[55]:
```
(26, 9)
```

26 filas y 9 columnas que se detallan a continuación.

In [41]:
```
df1.columns
```

Out[41]:
```
Index(['Tiempo', 'Tipo', 'Monto', 'Saldo_Inicial_antes_transaccion',
       'Nuevo_saldo_cliente', 'Balance_anterior_destinatario',
       'Nuevo_balance_destinatario', 'Es_fraude', 'Intentos_ilegables'],
      dtype='object')
```

El set de datos tiene:

26 Filas 11 Columnas

Tiempo:

Asigna una unidad de tiempo en el mundo real. Representa la hora y fecha en la que se realizó la transacción

Es_fraude:

Variable respuesta, donde 1 representa una transacción fraudulenta

Tip0:

Cash-in, Cash-out, débito, pago, transferencia

Monto:

Monto de la transacción

Nombre_cliente:

Cliente que inició la transacción

Saldo_Inicial_antes_transaccion:

Saldo inicial del remitente antes de la transacción

Nuevo_saldo_cliente:

Nuevo saldo del remitente después de la transacción

Nombre_destinatario:

Cliente destinatario de la transacción

Balance_anterior_destinatario:

Saldo inicial del destinatario antes de la transacción

Nuevo_balance_destinatario:

Nuevo saldo del destinatario después de la transacción

Es_fraude:

Variable respuesta, donde 1 representa una transacción fraudulenta

Tip0:

Cash-in, Cash-out, débito, pago, transferencia

Monto:

Monto de la transacción

Nombre_cliente:

Cliente que inició la transacción

Saldo_Inicial_antes_transaccion:

Saldo inicial del remitente antes de la transacción

Nuevo_saldo_cliente:

Nuevo saldo del remitente después de la transacción

Nombre_destinatario:

Cliente destinatario de la transacción

Balance_anterior_destinatario:

Saldo inicial del destinatario antes de la transacción

Nuevo_balance_destinatario:

Nuevo saldo del destinatario después de la transacción

Tip0:

Cash-in, Cash-out, débito, pago, transferencia

Monto:

Monto de la transacción

Nombre_cliente:

Cliente que inició la transacción

Saldo_Inicial_antes_transaccion:

Saldo inicial del remitente antes de la transacción

Nuevo_saldo_cliente:

Nuevo saldo del remitente después de la transacción

Nombre_destinatario:

Cliente destinatario de la transacción

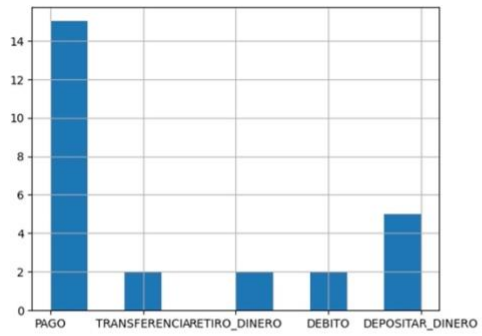
Balance_anterior_destinatario:

Saldo inicial del destinatario antes de la transacción

Nuevo_balance_destinatario:

Nuevo saldo del destinatario después de la transacción

Out[43]:
```
<AxesSubplot:>
```



Cuantos fraudes tenemos?

In [44]:
```
df1['Es_fraude'].value_counts()
```

Out[44]:
```
0    24
1     2
Name: Es_fraude, dtype: int64
```

En la anterior informacion nos dice que de los "26" clientes que realizaron algun tipo

de movimiento como "Transferencia", "Retirar dinero", "Depositar dinero", etc

De acuerdo a los datos, los fraudes se han presentan en

- RETIRO y
- TRANSFERENCIA

In [47]:
```
df1.groupby(['Tipo','Es_fraude'])['Es_fraude'].count()
```

Out[47]:
```
Tipo              Es_fraude
DEBITO            0             2
DEPOSITAR_DINERO  0             5
PAGO              0            15
RETIRO_DINERO     0             1
                  1             1
TRANSFERENCIA     0             1
                  1             1
Name: Es_fraude, dtype: int64
```

Distribucion del monto en las transacciones fraudulentas

In [48]:
```
fraude =  df1['Monto'].loc[df1['Es_fraude']==1.0]
print(fraude)
```

```
2    181.0
3    181.0
Name: Monto, dtype: float64
```

3) MATRIZ DE CORRELACION

In [49]:
```
correlation_matrix = df1.corr()
correlation_matrix['Es_fraude'].sort_values(ascending=False)
```

Out[49]:
```
Es_fraude                       1.000000
Nuevo_balance_destinatario     -0.094612
Balance_anterior_destinatario  -0.099604
Monto                          -0.168587
Saldo_Inicial_antes_transaccion  -0.183907
Nuevo saldo cliente            -0.186535
```

Intentos_ilegales:

Intentos ilegales. Un intento ilegal en este conjunto de datos es un intento de transferir más de 200.000 en una sola transacción

Tipo de transacciones

In [42]:
```
df1['Tipo'].unique()
```

Out[42]:
```
array(['PAGO', 'TRANSFERENCIA', 'RETIRO_DINERO', 'DEBITO',
       'DEPOSITAR_DINERO'], dtype=object)
```

Los tipos de fraude podria darse respecto al siguiente analisis de movimientos, cuya cantidad se especifica en la siguiente instrucción del modelo matematico.

In [56]:
```
df1.groupby(['Tipo'])['Es_fraude'].count()
```

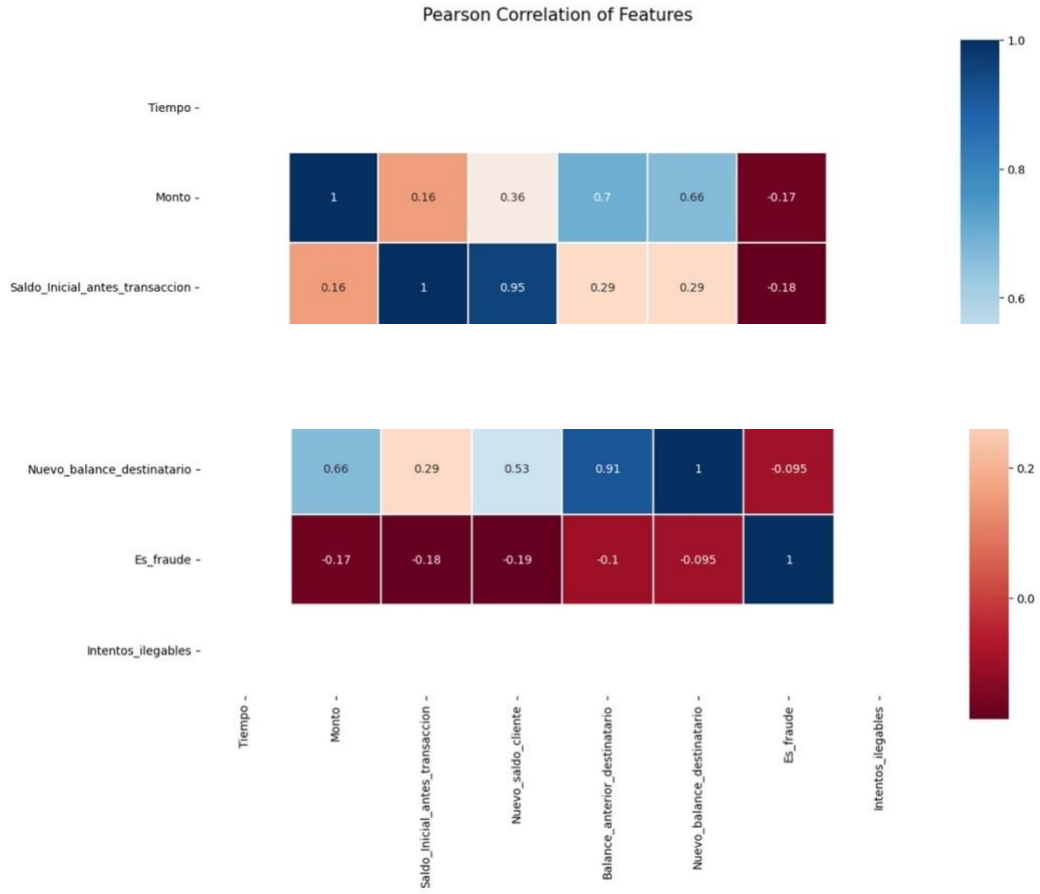
Out[56]:
```
Tipo
DEBITO               2
DEPOSITAR_DINERO     5
PAGO                15
RETIRO_DINERO        2
TRANSFERENCIA        2
Name: Es_fraude, dtype: int64
```

In [43]:
```
df1['Tipo'].hist()
```

```
Tiempo                              NaN
Intentos_ilegables                  NaN
Name: Es_fraude, dtype: float64
```

In [50]:
```
colormap = plt.cm.RdBu
plt.figure(figsize=(14,12))
plt.title('Pearson Correlation of Features', y=1.05, size=15)
sns.heatmap(correlation_matrix,linewidths=0.1,vmax=1.0,
            square=True, cmap=colormap, linecolor='white', annot=True)
```

Out[50]:
```
<AxesSubplot:title={'center':'Pearson Correlation of Features'}>
```



4) Fase de selección y entrenamiento del modelo

In [51]:
```
X = df1.drop(columns=['Es_fraude','Tipo']) # atributos de analisis (entrada de datos)

y = df1['Es_fraude'] # target o clase , es decir el referente para la guia
```

In [52]:
```
X_train, X_test, y_train, y_test = train_test_split(X, y, test_size=0.20, random_state=101)
```

Iniciemos creando un modelo matemático basado en el algoritmo Random Forest

Entropia= Caos , Impureza o desorden en la informacion de los datos

In [53]:
```
rf = RandomForestClassifier()
rf.fit(X_train, y_train)
train_pred = rf.predict(X_train)
```

In [61]:
```
print(" La precisión del modelo matemático para identificar el fraude en los movimientos estudiados es: ", accuracy_score(y_train, train_pred))
```

```
 La precisión del modelo matemático para identificar el fraude en los movimientos estudiados es:  1.0
```

5) CONCLUSIONES:

El modelo matemático es capaz de reconocer el 100% de los fraudes y cuando predice

también lo hace con un 100% de seguridad.

- Clemencia Elena Carranza Bravo

Del proceso algorítmico:

La construcción del algoritmo tuvo una efectividad de un 100 % debido al cumplimiento de los requisitos de calidad para el desarrollo.

a. Se identificó el problema: Se realizo la simulación de un caso para optimizar y controlar.
b. Se realizó la elección del tipo de algoritmo, tomando en cuenta el tipo de respuesta que se quería obtener.
c. Se identifico el mayor número de datos importantes, se rotulo y clasifico las variables independientes y dependientes.
d. Se formuló el modelo en el que se detalló los datos de entrada y el tipo de herramienta matemática a ser usada. Inmediatamente se construyó el algoritmo y se ensamblo los archivos informáticos.
e. Se comprobaron los resultados.
f. Finalmente se compiló el algoritmo matemático y se aplicó el proceso de reconstrucción de los hechos; para este efecto se acordó actividades detalladas en la bitácora de investigación.

Diseño de Acta de actuación en la escena del delito.

Acta de actuación para el responsable
Número Único de Registro del caso:
Ciudad Departamento Fecha Hora
LUGAR DE LOS HECHOS
Dirección
Barrio
Características
Hora de la ocurrencia de los hechos
PROTECCION DEL LUGAR DE LOS HECHOS
Acordonamiento SI NO
OBSERVACIONES DEL LUGAR DE LOS HECHOS
¿Hubo alteración del lugar de los hechos? SI NO
¿Por qué?
Intervinientes
Observaciones
INFORMACION OBTENIDA SOBRE LOS HECHOS (Una descripción breve)
SISTEMAS AFECTADOS Nombre Ubicación Observaciones Criticidad
ELEMENTOS IMPLICADOS
Marca Clase/Modelo Color TIPO Serial
TESTIGO DE LOS HECHOS
Nombres y Apellidos Identificación Datos de ubicación Observaciones adicionales
PRIMER RESPONDIENTE
Nombres y Apellidos Identificación Datos de ubicación Observaciones adicionales
¿Fue relevado? SI NO Fecha del relevo
Hora del relevo Firma
REGISTRAR PERSONA QUE REALIZA EL RELEVO
Nombres y Apellidos Identificación Datos de ubicación Observaciones adicionales
OBSERVACIONES
Fecha Hora del recibido Firma

ANEXO 2

ENTREVISTAS