Ordenamientos técnicos y metodológicos de las evidencias digitales forenses, como dato de prueba o descubrimiento probatorio en las investigaciones criminales

*Pedro Pablo Carmona Sánchez**

¿Por qué esta magnífica tecnología científica, que ahorra trabajo y nos hace la vida más fácil, nos aporta tan poca felicidad? La respuesta es esta, simplemente:

porque aún no hemos aprendido a usarla con acierto.

-Albert Einstein:*14/03/1894 Ulm, Alemania - 18/04/1955 Princeton, USA.*

Sumario: I. Introducción. **II.** Globalización y avance tecnológico. **III.** Seguridad informática. **IV.** Informática forense. **V.** Evidencia digital latente. **VI.** Fundamentación jurídica. **VII.** Procesamiento del escenario del delito o lugar de los hechos. **1.** Actuación en el lugar de los hechos. **2.** Obtención de la información dinámica o procesamiento. **3.** Generación de la evidencia digital forense. **4.** Análisis de la imagen digital forense. **5.** Datos de prueba, dictamen, informes de la evidencia digital.

Resumen: Dentro del mundo de la criminalística forense, hay pocos conceptos más importantes que los datos de prueba, los cuales cumplen la función indispensable de acreditar ciertos hechos como constitutivos dentro de una teoría del caso que contempla la comisión de un delito. Con el surgimiento de nuevas tecnologías, y la permanencia de servicios digitales en nuestras sociedades, este ensayo buscará explicar la definición, fundamentación jurídica, proceso de análisis y utilización como medio de prueba de las evidencias digitales latentes, que son aquellas que no se encuentran a simple vista en los dispositivos electrónicos.

* Doctor en Derecho por la Universidad Nacional Autónoma de México; maestría en Derecho "Ciencias Penales" por la UNAM; especialidad en derecho penal por la UP; especialidad en criminalística; licenciatura en Derecho por la UNAM.

Abstract: In the forensic and criminalistic universes, few concepts bear the weight of its importance as much as clues and case data, which serve the necessary purpose of relating a series of events within a certain case theory in which a crime was perpetrated. With the rise of new technologies by the hour, and the permanent character of said digital correspondence in our societies, this essay will seek to explain the definition, legal foundation, process of analysis and its use as future case data of latent digital evidence; that is, said evidence that is not easily findable in digital and electronic data.

Palabras clave: evidencias digitales latentes, indicios, datos y medios de prueba, TICs (tecnologías de la información y comunicación)

Key Words: latent or hidden digital evidence, clues, case data, test medium, TICs (information and communication technologies)

I. INTRODUCCIÓN

Conforme a las integraciones, conformaciones y clasificaciones jurídicas de las carpetas de investigación de delitos federales contemplados en el Código Penal Federal y la Ley Federal contra la Delincuencia Organizada, que se inician o instruyen en la Fiscalía Especializada de Investigación en Materia de Delincuencia Organizada (FEMDO) de la Fiscalía General de la República (FGR), así como en base a su forma y perfeccionamiento técnico-jurídico —apegados al Código Nacional de Procedimientos Penales para su judicialización ante el juez de control o de Garantías del Poder Judicial de la Federación—, lo importante y trascendental como una estrategia jurídica justificada es la aprehensión, percepción e identificación del indicio o bien, la evidencia. Como el material sensible y significativo para el esclarecimiento de los hechos, estos permiten la formulación, seguimiento, evaluación y replanteamiento del plan estratégico de justicia penal y, consecuentemente, la probable autoría, participación o responsabilidad de las personas.

Con los adelantos de las ciencias forenses, tratándose de la *evidencia digital latente*, o evidencia material probatoria, este dato de prueba o descubrimiento probatorio permite al fiscal especializado o agente del Ministerio Público de la federación, del fuero común o militar, poder acreditar, probar, comprobar o demostrar, como medio estratégico técnico, los elementos jurídicos o constitutivos del tipo específico del delito, los cuales son evidenciables procedimentalmente en la preservación, identificación, fijación, embalaje, etiquetamiento, documentación de entrega y recepción, por medio de una adecuada y reglamentada cadena de custodia. Con la identificación de indicios y evidencias, como datos y medios de prueba idóneos, estos permiten demostrar la verdad real, la verdad técnico-científica, o la verdad lógica jurídica que se busca en la investigación criminal.

El erudito doctor Edmund Locard[1] (Saint-Chamón, Ródano —Alpes, 13 de diciembre 1877— Lyon, 4 de mayo 1966) es considerado creador de la criminalística universal. Doctor en medicina y derecho, director del Laboratorio de Policía Técnica de Lyon, Francia; fue quien perfeccionó líneas de la investigación científica y estableció que un criminal, a su paso por el escenario del crimen o lugar de los hechos, circunstancialmente o menudamente se encuentra condicionado por el *principio de intercambio:* siempre en su paso deja algo. En su camino por la escena deja algún indicio o evidencia o se lleva algo del mismo lugar, como material sensible y significativo; esto como prueba material, descubrimiento probatorio o circunstancial deberá de observarse, fiarse, identificarse y embalarse para trasladarse en cadena de custodia al laboratorio de criminalística, sitio donde los expertos o especialistas determinarán las características y particularidades de la evidencia en comento.

En esa virtud, para el tratadista doctor en derecho y juez de instrucción Hans Gross de Graz[2] (9 de diciembre 1847- 5 de diciembre 1915) considerado como el padre de la criminalística y su método científico, deja en su obra escrita de 1893, intitulada: *Handbuch fur Untersuchungsrichter als Systems der Kriminalistik, Manual del Juez de Instrucción, Todos los Sistemas de Criminalística,* la siguiente redacción (Gross, 1900: pág. 6, traducción de Arredondo) se redactó lo siguiente:

> ...el delincuente ha podido antes y después de cometer el delito, utilizar cuantos medios le sugiera su astucia e instinto de conservación para burlar la acción investigadora del Estado y eludir la pena; en tanto que el juez, con los datos incompletos que le suministra el hecho realizado, se ve en la necesidad de dejar la incógnita del proceso, que cuidadosamente ocultan, de un lado la fatalidad y de otro los esfuerzos del criminal, razón por la que, le es indispensable suplir estas deficiencias, no solo por el impulso poderoso de su talento, sino también por los consejos de la experiencia, propia o ajena, que a esta tendrá que acudir en defecto de la primera, ya que sin ella rara vez podrá llevar a término feliz la empresa que la sociedad confía...

Este manual enfatiza o destaca la importancia del perfil, así como las características personales que deben poseer los sabios investigadores especializados de un crimen o delito, como son: objetividad, diligencia, perseverancia, conocimientos de la naturaleza humana y la necesidad de recurrir a expertos de las ciencias penales o diciplinas científicas forenses, que permitan ayudar en el perfeccionamiento de la investigación criminal.

---

1 Locard Edmund, *Manual de Técnicas Policiacas,* doctor en medicina y derecho; director del Laboratorio de Policía Técnica de Lyon, Francia; con prólogo de D. Aitor M. Curiel López de Arcaute, Editorial José Monteso, 978-92-0-377388-1, Barcelona España, 1935.

2 Gross Hanns de Graz, *Manual del Juez,* para los jueces de instrucción, municipales, alcaldes, escribanos, oficiales, agentes de la policía, traducido del alemán, prologo y notas por D. Máximo de Arredondo, juez de primera instancia del Tribunal Contencioso, Editorial La España Moderna, Madrid. 1983.

II. GLOBALIZACIÓN Y AVANCE TECNOLÓGICO

Las infraestructuras de medios digitales y la globalización de la información tecnológica se han multiplicado exponencialmente, así como también la capacidad de conocer el crecimiento del volumen de datos que se cruzan diariamente por organizaciones criminales se ha incrementado. Esta información almacenada en equipos electrónicos tecnológicos es la evidencia informática de procesamiento de datos, fundamento principal que se intercambia cotidianamente entre personas, grupos, organizaciones criminales y sociedades en todo el mundo. Por todo ello, es necesario y fundamental que, durante las estrategias jurídicas estructuradas de una investigación en materia penal, se utilice necesariamente un mayor volumen de información sensible y significativa en los intercambios de equipos intra e interinstitucionales.

Tratándose del formato digital electrónico de cualquier organización criminal estratégica y operacional que se circule, difunda y publique en redes informáticas, este constituye un entorno o biósfera, conformado por redes privadas locales y globales, las cuales son materia de cultivo para las organizaciones criminales. Esto, tratándose de materias como delincuencia organizada; y/o sujetos o individuos que se involucran asidua o frecuentemente en actos delictuosos. En esa virtud, resulta necesario seguir e investigar a este problema social pegado como la sombra al cuerpo, dependiente en relacionarse cotidianamente con las comunicaciones por vía electrónica con equipos sofisticados de nueva generación, los cuales se deberán analizar y valorar en sus distintas fases. Estas comprenden desde la generación de datos, el almacenamiento y registro, hasta la administración, el envío y validación de la más mínima información, al poder descubrirse los vínculos en cada uno de estos procesos técnicos analíticos metodológicos, pueden convertirse en ventanas de vulnerabilidad o elementos de convicción para ser demostrados como datos de prueba o descubrimientos probatorios; esto a manera de relaciones o enlaces entre sujetos primo delincuentes y otros malhechores, expertos en grupos delincuenciales con organizaciones criminales.

Ante estas amenazas sociales, resulta conveniente por parte del Estado, estructurar o construir el destino sensitivo de la información como indicio o material sensible y significativo. A través del tamiz o filtro del análisis de expertos en informática, TICs, la vulnerabilidad de los operadores y los medios de trasmisión utilizados, el valor estratégico y la legalidad de los mensajes, sus características, particularidades e intereses intrínsecos de sus destinatarios, así como su capacidad organizacional para poder controlar la información circulante movible o almacenada en la nube, se obtendrán elementos probatorios indubitables e incuestionables de gran utilidad en el proceso penal.

El objeto y alcance de la *digitalización* es la información sensible e indagación de *textos, imágenes, sonidos, animaciones*, trasmitidos por los mismos medios al estar

representados en un formato único universal. En algunos casos, los sonidos (a transmisión tradicional) se hacen en la forma analógica y, para que puedan comunicarse de forma consistente por medio de las redes telemáticas, es necesario su trascripción a una codificación *digital*. Con ese propósito, y tomando en cuenta que la mayor parte de la información que se maneja en nuestros tiempos modernos es en formatos digitales, resulta necesario contar con equipos de última generación o de punta, así como del personal especializado experto con capacidad de análisis de inteligencia *digital*, con soportes técnicos-metodológicos para poder obtener objetivamente los indicios, datos de prueba y descubrimientos probatorios y evidencias de la información o evidencia digital informática, como elementos de convicción para confirmar la participación del sujeto y la organización criminal.

III. SEGURIDAD INFORMÁTICA

Uno de los hechos más apreciables, destacados o manifiestos en el entorno nacional e internacional es la creciente relevancia y preminencia de la informática forense, dado por su relación con sujetos como sociedades, universidades, corporaciones, empresas privadas, estatales y gubernamentales. Dentro de la estrategia jurídica diseñada en las líneas de investigación técnica científica, la informática forense permitiría acreditar o demostrar la verdad real o histórica, así como la verdad jurídica; existe el ejemplo empírico de conocer los *modus operandi* de las organizaciones delictivas, como la delincuencia organizada en materia federal. Paradójicamente, estas organizaciones criminales cada vez son más vulnerables frente a las dificultades legales de tipo criminales, como también la fuga de información a través de sus sistemas de cómputo o equipos electrónicos.

Esta realidad o contexto, puede llegar a ser crítica, diatriba o invectiva si consideramos que actualmente la mayor parte de la información (de manera estratégica y operativa) de empresas oficiales, públicas o gubernamentales como personales privadas o particulares, exponencialmente se incrementa en los medios de comunicación electrónicos —estas rebasan recientemente el 98 % del censo encuestado—, la cual se procesa preferentemente en los medios electrónicos digitales, aunque su formato final sea impresión en papel y tinta. Por su parte, estas organizaciones o formaciones criminales con la finalidad de poder proteger y salvaguardar sus propias unidades de cómputo con las cuales operan las redes interrelacionadas o interconectadas, cimentan, establecen, diseñan o construyen barreras con blindajes electrónicos, escudos o protecciones digitales. Esto con el objetivo de proteger y resguardar la base de datos de la información sensible y latente, como también, tratar de impedir que cualquier otra persona ajena a la organización pueda acceder, consentir o permitir acceso a sus equipos personales o privados (institucionales o gubernamentales) en los cuales yace, reposa o se encuentra latente la propia información que se busca durante la propia pesquisa o requisa de la investigación.

Resulta importante señalar que se requieren expertos conformados por equipos multidisciplinarios e interdisciplinarios de policías ministeriales federales y peritos profesionales especializados en informática forense, que cuenten con el dominio de las técnicas y metodologías específicas o sensibles latentes que permitan explorar de forma exhaustiva, detallada, sistemática y pormenorizada, las informaciones almacenadas u ocultas y que sus poseedores o usufructuarios realizan a través de equipos computarizados o por equipos de tecnologías de punta personales, como celulares o medios electrónicos.

Con la finalidad de poder controlar la información que se recibe y se envía de los diferentes dispositivos electrónicos por parte de particulares o privados, así como de instituciones gubernamentales o de grupos de organizaciones criminales, existen dispositivos, mecanismos, módulos o componentes que permiten proteger estos equipos de cómputo electrónicos, a fin de circunscribir, restringir o limitar la presencia de hackers o visitantes no deseados. Sin embargo, con los avances tecnológicos contemporáneos y con la fragilidad o laxitud del factor humano, se generan ventanas de vulnerabilidad o fragilidad en los grupos de delincuentes malhechores que conforman e integran las diferentes organizaciones criminales, las cuales laceran, corroen o carcomen nuestras familias, estirpes o sociedades.

IV. INFORMÁTICA FORENSE

El análisis digital en las ciencias forenses consiste en la aplicación técnica científica y de análisis especializados de expertos que permiten preservar, identificar, fijar, embalar y, en cadena de custodia oficialmente, analizar y presentar evidencias o datos de prueba que sean determinantes y comprobables dentro de una estrategia jurídica en un proceso legal.

En 1984, el FBI conforma o integra el *Magnetic Media Program*, que más tarde en 1991, será el *Computer Análisis and Response Team* (CART). En 1988 se crea la *International Association of Computer Investigative Specialists* (IACIS) que certificará, previa capacitación, a los profesionales gubernamentales en el *Certified Forensic Computer Examiner* (CFCE), una de las más prestigiosas y reconocidas en el ámbito de las Ciencias Forenses. Asimismo, se crea un programa de *Seized Computer Evidence Recovery Specialists* (SCERS), con el objetivo de formar especialistas o expertos en la materia informática. En 1995 se crea la *International Organization on Computer Evidence* (IOCE) con el propósito y el objetivo de mantener un punto de encuentro entre especialistas en la preservación, identificación, fijación y embalaje de la evidencia electrónica y el intercambio o la reciprocidad de la información sensible y latente. En 2001 surge o germina la *Digital Forensic Research Workshop* (DFRWS), como una base de datos o terminal especializada de debate y discusión internacional para compartir información de grupos delincuenciales o células criminales.

Con la estructuración académica de la carrera de ciencias forenses por la Universidad Nacional Autónoma de México, en su columna vertebral se cuenta con la informática forense, materia fundamental y necesaria para la formación de estudiosos que buscan saber y conocer los avances de la ciencia y del conocimiento moderno de las técnicas de la información y de la comunicación, con una habilidad técnica y metodología de investigación objetiva y cuantitativa que permita o sirva en las investigaciones en los cuales se consuman o ejecutan hechos constitutivos de delitos graves de alto riesgo. Esto, con la utilización de equipos con tecnologías de punta de última generación y sus sistemas de cómputo en los cuales se puedan obtener material sensible y significativo que permita conocer, descubrir y demostrar la evidencia digital latente u oculta como dato de prueba o descubrimiento probatorio, tanto para las personas particulares como de instituciones y organizaciones criminales con alcances distorsionados o retorcidos malhechores.

Esta disciplina especializada, auxiliar de las ciencias penales, tiene como objetivo principal la pesquisa o búsqueda de la información estratégica en el descubrimiento de evidencias digitales en los sistemas y redes informáticos, que en esencia se refiere al análisis, estudio y evaluación a fondo de la información digital oculta o latente que circula en los equipos, plataformas y sistemas de personas delincuentes que formen parte de un grupo criminal. Como la última fase de la informática forense que permita a estos expertos emitir las interpretaciones y consideraciones pertinentes al caso concreto, se deben establecer líneas de investigación de inteligencia. Posteriormente, estos expertos harán sus hallazgos del conocimiento de los elementos de la Agencia de Investigación Criminal en materia federal, quienes son los responsables de diseñar y estructurar las líneas de investigación fundamentales con la finalidad de ofrecerlos al fiscal especializado o agente del Ministerio Público de la federación, del fuero común o militar, quienes al conocer la importancia de la evidencia digital latente, la evaluarán, para usarlos como dato de prueba o descubrimiento probatorio que sea admitida en la judicialización o en la teoría del caso dentro del juicio oral por delitos cibernéticos, violaciones sexuales, trata de personas o delincuencia organizada.

En nuestro país, este tipo de estrategias o procesos de líneas de investigación, actualmente, ya se cuentan en la operatividad especial, a cargo de la Fiscalía Especializada en Materia Federal en Delincuencia Organizada. Estas deben sustancialmente perfeccionarse, con la finalidad de que todo investigador e integrador de una carpeta de investigación, pueda ir o caminar en la ruta del estudio del crimen con un paso adelante del delincuente, malhechor o probable responsable de la delincuencia organizada, esta última definida en el artículo 2° de la Ley Federal contra la Delincuencia Organizada como sigue:[3] *cuando tres o más personas se organicen de hecho*

[3] Cámara de Diputados del H. Congreso de la Unión, Ley Federal contra la Delincuencia Organizada, publicado en el *Diario Oficial de la Federación* DOF 20-05-2021.

para realizar, en forma reiterada y permanente, conductas que por sí o unidas a otras, tienen como fin o resultado cometer alguno o algunos delitos, serán sancionados por ese solo hecho, como miembros de la delincuencia organizada.

El laboratorio de criminalística en materia federal como en el fuero común y militar deberá contar con un área especializada en informática forense, con el objetivo de poder analizar y examinar cada uno de los equipos en los cuales puedan existir información almacenada relevante, de evidencia digital que permita descubrir la información latente que se busca: el tiempo, modo y lugar en el que un sujeto actúe o participe en la comisión del ilícito que se investiga. Debería también contar con una infraestructura o red nacional e internacional, emitiendo trabajos con el mayor nivel de profesionalismo, los cuales deberán mantener el sigilo, la discreción y confiabilidad que se requieren en estas responsabilidades.

V. EVIDENCIA DIGITAL LATENTE

El término refiere a un indicio o material sensible y significativo oculto, el cual después de analizado o examinado detalladamente, e identificado dicha información oculta, se convierte en una evidencia material. A través del estudio y análisis especializado de expertos en tecnologías de la información y comunicación dicha evidencia material permite conocer y obtener, con certeza, esa evidencia física material demostrable, sensible, visible, tangible, perceptible, así como otras formas de evidencia identificativas (DNA, huellas digitales, dispositivos o componentes de computadoras y equipos de tecnologías de punta para las comunicaciones privadas o personales, institucionales, gubernamentales o de organizaciones criminales). La evidencia digital, al ser objetivada técnica científicamente por expertos, así como preservada, identificada, fijada, procesada y analizada previa cadena de custodia, deberá aprovecharse al máximo en los distintos escenarios. En cada uno de ellos existe una estrategia jurídica especial o diferente, respecto a lo que se pretende obtener como una calidad probatoria sensible y significativa, si se busca precisión en el análisis especializado con tecnologías y metodologías objetivas y cuantitativas, aplicadas durante el procedimiento.

Estos procesos fueron estructurados, diseñados o constituidos con la finalidad de preservar y mantener la integridad del material sensible y significativo como evidencia digital latente, con una sistemática técnica científica aceptable o aprobada para establecer la requisa y la admisibilidad del dato de prueba o descubrimiento probatorio. En los procesos legales en materia penal, este material en forma de evidencia digital se debe encontrar en sintonía con la norma ISO/IEC 27037:2012, la cual indica, entre otras cosas, cómo generar herramientas determinantes y protocolos de análisis digital forense. Esta norma, en esencia, permite proporcionar los procedimientos o pautas adecuadas que permitan constituir el manejo adecuado de la evidencia digital latente, sistematizando o normalizando la preservación, la iden-

tificación, la fijación y la recolección y embalaje de la misma en cadena de custodia oficial y legalmente, con la finalidad de poder mantener la integridad de la evidencia digital latente, de acuerdo con los principios de la ISO/IEC 27037:2012: *relevancia*, *confiabilidad* y *suficiencia*.

Una particularidad importante del trato que se le da a la evidencia digital latente, se relaciona con la manera en que se busca recuperar dicha evidencia, antes intentos por hackers de la delincuencia organizada de destruir esta. Esta información tiene el riesgo de poder ser extraída en original, o bien duplicada de manera exacta o idéntica. No obstante, resulta relativamente sencillo identificar si la evidencia digital latente haya sido alterada en comparación con la original; en estos casos, la autoridad también cuenta con la tecnología para recuperar o recobrar la información. Asimismo, conforme al principio de suficiencia e idoneidad de la evidencia digital, debe haber un constante mejoramiento de los procedimientos para las investigaciones; no solo durante las pesquisas de los distintos dispositivos tecnológicos analizados en el escenario de un crimen, sino también con las técnicas y metodologías forenses en la búsqueda y localización de la evidencia digital.

Con ello, durante la estrategia jurídica diseñada o delineada, esto determinará el tipo de análisis o líneas de investigación que deberán establecerse con el objetivo procedimental de obtener los indicios o evidencias ocultas o latentes, los cuales deberán ser utilizadas como datos de pruebas o descubrimientos probatorios, y con las cuales se sustentará la hipótesis principal, determinante en la teoría del caso investigado. Con este propósito, se categorizarán cada uno de los indicios o evidencias digitales latentes como datos de prueba o descubrimiento probatorio, para poder distinguir entre el elemento hardware y la información contenida en éste, también denominada evidencia electrónica y digital, respectivamente. Este diseño o delineación facilita el diseño de las metodologías y procedimientos adecuados en el manejo, análisis y estudio de cada tipo de indicio o evidencia latente identificada, consiguiendo con ello un paralelismo entre el escenario físico y consecuentemente el entorno digital.

Resulta importante tener correctamente establecidos los procedimientos de identificación, fijación, recopilación y almacenamiento de las evidencias en el escenario del crimen o lugar de los hechos, así como la cadena de custodia de los mismos oficial y legamente. Acorde a esta, las evidencias deberán ser trasladadas al laboratorio de criminalística especializado en *evidencias digitales*, sitio en el cual los expertos en electrónica y equipos de tecnologías de punta determinarán las técnicas y métodos, a efecto que esos indicios inicialmente se conviertan en evidencias digitales latentes. Con el fin de que no sufran alteraciones durante el procedimiento de análisis, los informáticos forenses especializados basarán sus indagaciones periciales y análisis forenses digitales en normas y guías publicadas al respecto, tales como RFC *(Request for Comments)*, e ISO *(International Organization for Standardization)*.

La norma ISO/IEC27037,[4] "Guía oficial para la Identificación, Recolección, Adquisición y Preservación de Evidencias Digitales", es un manual de procedimientos que proporciona los lineamientos y directrices procedimentales para localizar e identificar evidencias digitales en teléfonos móviles,[5] tarjetas de memoria, dispositivos electrónicos personales, sistemas de navegación móvil, cámaras digitales y de video, redes TCP/IP, las cuales una vez identificadas como una *evidencia digital,* pueden ser utilizadas como dato de prueba o descubrimiento probatorio.

Esta norma proporciona orientación para los siguientes dispositivos:

1. Medios de almacenamiento digital, como discos duros, discos ópticos, cintas, que se suelen emplear en equipos de computadoras y sistemas informáticos.
2. Teléfonos móviles, PDAs (asistente personal digital), dispositivos personales electrónicos, tarjetas de memoria.
3. Sistemas de Navegación Georreferenciados (GPS).
4. Equipos de conexión de red.
5. Cámaras digitales y de video.
6. Redes TCP/IP y otros protocolos digitales.
7. Todos aquellos dispositivos con funciones similar.

Durante todas las investigaciones para las obtenciones de las *evidencias digitales latentes* se requiere fundamentalmente que se establezcan los procedimientos e instrucciones estructurados o constituidos en los tres principios específicos contenidos en la norma ya mencionada:

A. La ***relevancia***: es considerada como una condición técnicamente jurídica, en la cual se establecen elementos que son acertados o pertinentes a la situación o contexto que se analiza e investiga, con el objetivo de probar la hipótesis planteada con relación a los hechos que se investigan.

B. La ***confiabilidad***, como una característica principal, la cual busca validar la repetibilidad y auditabilidad de un proceso aplicado para la obtención de una evidencia digital latente, por lo que la evidencia que se extrae o se obtiene es la que es o la que debe ser; un tercero procedimentalmente deberá obtener resultados iguales o similares verificables o comprobables.

C. La ***suficiencia***. Como tercer principio, se encuentra relacionado con la completitud de pruebas informáticas; es decir, en las evidencias recolectadas y analizadas se tienen elementos suficientes por medio de los cuales expertos especializados (sujetos

[4] Roatta Santiago, Casco María Eugenia, Fogliato Martín, *El Tratamiento de la Evidencia Digital y las Normas ISO/IEC 2737: 2012,* Facultad Tecnología Informática, Universidad Interamericana, Facultad de Derecho de la Universidad de Rosario, Córdova.

[5] Gómez, L.S., "Protocolo de Actuación para Pericial Informáticas", Poder Judicial de la Provincia, Ley Provincial 1339-2010, *Boletín Oficial de la Provincia de Santa Fe,* noviembre 2010.

a la experticia y formalidad del docto en informática forense) recaben, aseguren, y preserven los elementos materiales sensibles latentes, como material probatorio sobre medios digitales, para poder sustentar las hipótesis del hecho criminal investigado.

En la estrategia jurídica diseñada y estructurada durante una investigación criminal, pueden encontrarse distintos dispositivos tecnológicos que fueron previamente secuestrados para establecer un hecho determinado. En estos casos, el fiscal federal o agente del Ministerio Público de la federación, del fuero común o militar, juez o magistrado deberán ser informados y orientados correctamente sobre la certeza o la veracidad que guarden estos dispositivos tecnológicos. Por medio de la demostración de los indicios, y posterior a haber sido analizados técnico-científicamente, es como se consigue que la *evidencia digital* sea determinante y concluyente a la verdad que se busca durante la investigación criminal.

Con los adelantos de las comunicaciones y tecnologías de nuestros tiempos, así como la *evidencia digital* latente y su omnipresencia, resulta paradójico o raro que, en la comisión o perpetración de un crimen o delito, no se encuentren asociados mensajes de datos guardados y trasmitidos por medios informáticos. De encontrarse estos, un policía de la Agencia Federal de Investigación Criminal en materia federal, del fuero común o militar entrenado, con una experiencia y dominio de las líneas de investigación, puede usar el contenido del mensaje de datos localizado en el equipo electrónico, que le permitirá descubrir la conducta del infractor o malhechor y mediante el cual puede hacer un perfil, sombra o silueta de su actuación relacionada bien a sus actividades personales, individuales, o por pertenecer a grupos criminales.

Dentro de los equipos electrónicos e informáticos que se contemplan para la obtención de evidencias digitales, se cuentan los siguientes:

A. Computadora de escritorio
B. Computadora portátil
C. Estación de trabajo
D. Hardware de red
E. Servidor (aparato que almacena o transfiere datos electrónicos por Internet)
F. Teléfono celular
G. Teléfono inalámbrico
H. Equipo o aparato para identificar llamadas
I. Localizador -beeper
J. "GPS" (aparato que utiliza tecnología satélite capaz de ubicar geográficamente a persona o vehículo que lo opera)
K. Cámaras de video
L. Sistemas de seguridad
M. Memoria "flash" (pequeño dispositivo que puede conservar hasta 4 gigabytes de datos o 4, 000 000 000 bytes de información)

N. "Palm" (asistente personal electrónico que almacena datos y conectividad inalámbrico con internet)
O. Juegos electrónicos (su unidad de datos) o la memoria de otro aparato
P. Sistemas computarizados dentro de vehículos y dentro de su sistema operativo
Q. Impresoras
R. Copiadoras
S. Grabadoras
T. Video reproductores de DVD
U. Duplicadora de discos
V. Discos, disquetes, cintas magnéticas
W. Aparatos ilícitos, tales como los equipos que capturan el número de celulares más cercanos para después copiar su información en otros teléfonos (también se les llama *sniffers* o decodificadores)

VI. FUNDAMENTACIÓN JURÍDICA

A. Ordenamientos legales:

- Constitución Política de los Estados Unidos Mexicanos, CPEUM
- Ley General del Sistema Nacional de Seguridad Pública
- Código Nacional de Procedimientos Penales
- Código Penal Federal
- Códigos Penales de los Estados de la República Mexicana

B. Instrumentos internacionales:

- Declaración Universal de los Derechos Humanos
- Convención Americana sobre los Derechos Humanos
- Convención de Palermo sobre Delincuencia Organizada Transnacional
- Convención de las Naciones Unidas contra la corrupción, (ONU)
- Convención Internacional para la protección de personas contra las desapariciones forzadas
- Convención contra la tortura y otros tratos crueles, inhumanos y degradantes
- Códigos de conducta para funcionarios encargados de hacer cumplir la ley
- Manual de la escena del delito y las pruebas materiales (debe sensibilizarse también al personal no forense sobre su importancia)

C. Leyes locales:

- Constituciones Estatales
- Leyes relacionadas con la seguridad pública, y las instituciones policiales de las entidades federativas

- Leyes Orgánicas de las fiscalías generales de justicia de los Estados de la República Mexicana
- Códigos penales de cada una de las entidades federativas

D. Acuerdos e instrumentos:

- Lineamientos L/001/2021 de la Fiscalía General de la República[6]
- **Acuerdo A/009/2015** de la Procuraduría General de la República,[7] por el cual se establecen las bases y directrices que deberán observar los servidores públicos que intervengan en materia de cadena de custodia
- Protocolo Nacional de Actuación de Primer Respondiente
- Guía Nacional de Cadena de Custodia
- Manual de la Evidencia Digital, Proyecto de Apoyo al Sector Justicia[8]
- Manual de Manejo de Evidencias Digitales y Entornos Informáticos[9]

VII. PROCESAMIENTO DEL ESCENARIO DEL DELITO O LUGAR DE LOS HECHOS

Los policías investigadores pertenecientes a la Agencia Federal de Investigación Criminal, de la policía de investigación ministerial, local o militar, en compañía de los peritos especializados o técnicos en equipos multidisciplinarios e interdisciplinarios, que se apersonen o arriben primero a la escena del crimen, tienen responsabilidades, las cuales se resumen de la siguiente forma:

A. Observe y establezca los parámetros de la escena del crimen: El primero en llegar al lugar de los hechos, deberá establecer si el delito está o se encuentra en progreso, luego tendrá que tomar notas de las características y particularidades físicas del área circundante, preservándolo correctamente. Para los investigadores forenses, esta etapa deberá ser extendida a todo sistema de información y de red que se encuentre dentro de la escena.

B. Inicie las medidas de seguridad: El objetivo fundamental o principal de toda investigación es la seguridad de los investigadores intervinientes y de la escena. Si uno con su observación establece una situación insegura dentro de la escena del delito, deberán de tomarse las medidas que

---

6 Gertz Manero, Alejandro, *Lineamiento L/001/2021, para el acceso a los servicios y visitas de información en la herramienta informática, de analistas de la Fiscalía General de la República,* 5 junio de 2021.

7 *Guía Técnica de Cadena de Custodia de Evidencia Digital,* Unidad de Investigaciones Cibernéticas y Operaciones Tecnológicas de la Procuraduría General de la República, México, junio 2018.

8 *Manual de Evidencia Digital, Proyecto de Apoyo al Sector Justicia,* American Bar Association Rule of Law Iniciative, ABA ROLI, Perú.

9 Acurio del Pino Santiago, *Manual de Manejo de Evidencias Digitales y Entornos Informáticos;* Director Nacional de Tecnologías de la Información, 2009.

resulten necesarias o pertinentes para poder corregir dicha situación. Se deberán de tomar las medidas y acciones necesarias a fin de evitar riesgos eléctricos, químicos o biológicos, así como cualquier actividad criminal.

C. Facilite los primeros auxilios: Siempre se deben tomar las medidas adecuadas para precautelar la vida de las posibles víctimas del delito. El objetivo es poder brindarles el cuidado y la atención médica por el personal de emergencias, así como preservar los indicios como material sensible y significativo (que luego podría fungir como posible evidencia).

D. Asegure físicamente la escena o lugar de los hechos: Es crucial, durante una investigación de tipo criminal, apartar, alejar, retirar o separar a todas las personas extrañas o ajenas a la misma; el objetivo principal es el de prevenir el acceso no autorizado de personas intrusas a la misma, evitando así necesariamente las posibles alteraciones y/o contaminación de indicios y evidencias, o de su posible modificación del escenario de los hechos.

E. Asegure físicamente las evidencias: Este momento procedimental o paso es muy importante, a fin de identificar, fijar y etiquetar en cadena de custodia,[10] los indicios sensibles o las evidencias para ser trasladadas al laboratorio de criminalística para su estudio y análisis especializado. En este caso, se aplican los principios, manuales, las técnicas y metodologías correspondientes a cada evidencia digital latente. Esto deberá ser efectuado por personal adiestrado o entrenado en el procesamiento de manejar, guardar, y etiquetar cada una de las evidencias.

F. Entrega de la escena del crimen o lugar de los hechos: Después de que se han cumplido con todas las etapas anteriormente descritas, el lugar de los hechos o la escena puede ser entregada a las autoridades, que se harán cargo de esta. Lo esencial de esta etapa es poder verificar que todos los

[10] La *cadena de custodia* es un sistema de aseguramiento que, basado en el principio de la mismidad, tiene como fin garantizar la autenticidad de la evidencia que se utiliza como prueba dentro del proceso. La información mínima que se maneja en la cadena de custodia, para un caso específico, es la siguiente: a) Una hoja de ruta, en donde se anoten los datos principales sobre la descripción de la evidencia, fechas, horas, custodios, identificaciones, cargo y firmas de quien recibe y quien entrega; b) Recibos personales que guarda cada custodio y donde están datos similares a los de la hoja de ruta; c) Rótulos que deben estar pegados a los envases de las evidencias, Ejem. a las bolsas de plástico, sobres de papel, sobres de manila, frascos, cajas de cartón etc.; d) Etiquetas que deben contener la misma información que los rótulos, pero van atadas con una cuerdita a bolsas de papel Kraft, o a frascos o a cajas de cartón o a sacos de fibra; e) Libros de registro de entradas y salidas, o cualquier otro sistema informático que se deben llevar a los laboratorios de criminalística o de análisis especializados, así como a las oficinas de los fiscales o agentes del Ministerio Público de la federación, del fuero común o militar, elementos de la agencia de investigación criminal de la fiscalía general de la república, o peritos especializados.

indicios y las evidencias del caso en estudio se hayan observado, preservado e identificado, fijado, etiquetado, recogido y almacenado en forma correcta.

G. Elabore la documentación de la explotación de la escena o del lugar de los hechos: Es indispensable para los investigadores documentar correctamente cada una de las etapas de este procedimiento, a fin de tener una completa bitácora de los hechos sucedidos o perpetrados durante la explotación de la escena del delito, las evidencias encontradas y su posible relación con los sospechosos.

Si se tiene la finalidad de establecer y utilizar las tecnologías de la información para el tratamiento de recursos informáticos o evidencia digital, en apego al marco constitucional y normativo, y que estas auxilien en la integración procedimental de las investigaciones, dichas investigaciones deben estar conforme a los lineamientos para la obtención y tratamiento de los recursos informáticos y/o evidencias digitales del Poder Judicial de la Federación del Consejo de la Judicatura Federal de la SCJN.[11]

1. Actuación en el lugar de los hechos

El personal especializado del área de tecnologías de la información, conformado al menos por dos personas autorizadas, se deberá de constituir o apersonar en el o los lugares, y su estrategia será con el objetivo de poder identificar los recursos informáticos y sus poseedores, indicando lugar, hora, fecha, nombre, así como la interacción posterior y su resguardo específico o determinado. Los objetivos generales son las acciones de todo servidor público de la federación (locales y municipales). Principalmente, refiere a aquellos que participen responsablemente y den respuestas a incidentes o sucesos en los cuales se le dé la importancia de preservar elementos materiales sensibles probatorios relacionados con el entorno de la *evidencia digital*. Esto tiene la finalidad de poder procesar dichas evidencias correctamente, para su identificación o reconocimiento y recopilación, con la finalidad de garantizar la mismidad y autenticidad dentro de una cadena de custodia oficialmente estructurada. Así, en su momento procesal oportuno, podrán ser incorporados como datos de prueba o descubrimiento probatorio en el proceso penal.

Dentro de los objetivos específicos mencionados, corresponden fundamentalmente a las *evidencias digitales* los que se enuncian a continuación:

A. Homologar las actuaciones de los servidores públicos federales, locales o militares para el debido manejo de los indicios o evidencias como elementos materiales probatorios digitales.

[11] Poder Judicial de la Federación, Consejo de la Judicatura Federal de la SCJN, Lineamientos para la obtención y tratamiento de los recursos informáticos y/o Evidencias Digitales, junio 2016.

B. Describir o relatar los lineamientos básicos para el uso de la implementación de la guía de actuación, interviniendo en el desempeño con eficiencia y experticia como servidores públicos responsables que intervengan o estén en contacto con el procesamiento de los indicios o evidencias materiales probatorios digitales.

C. Estandarizar y ajustar la ejecución durante el manejo de los indicios o evidencias latentes como elementos probatorios digitales desde su localización, durante la observación, reconocimiento, identificación, fijación y embalaje y transporte en cadena de custodia, hasta su disposición final en el laboratorio de criminalística especializada en evidencias digitales.

D. Los actores intervinientes en estas diligencias ministeriales federales, locales o militares pueden ser los siguientes:

a) Primer respondiente
b) Policía
c) Policía de investigación
d) Perito profesional especializado
e) Personal facultado o designado para el traslado
f) Personal especializado en informática digital
g) Encargado de bodegas de indicios o evidencias o cuerpos del delito
h) Fiscal federal o agente del Ministerio Público del fuero común o Militar

Para el análisis en el lugar de la investigación, es necesario realizar una imagen forense, y posteriormente otra en el laboratorio de criminalística especializado de tecnologías de la información. Consecuentemente, los especialistas, conformados por personal experto, procederán con lo siguiente:

- Asegurarse y verificar las condiciones de seguridad del escenario, con la finalidad de poder armonizar las actividades y uso del equipo necesario:
  - Guantes,
  - Pulseras antiestéticas,
  - Cámara fotográfica,
  - Bolsas antiestéticas,
  - Cables UTP,
  - Hule espuma,
  - Dispositivo duplicador forense,
  - Laptop con Software forense especializado, y
  - Medios de almacenamiento debidamente formateados.
  - Realizar un reporte fotográfico de todas las actividades previas y durante la recolección de la *evidencia digital*.
  - General una imagen forense de los recursos informáticos o *evidencias digitales*.
  - Sellar cada entrada o puerto periférico con cintas.
  - Identificar con etiquetas y registrar los recursos informáticos o *evidencia digital*.

- Embalar, preferentemente en bolsas antiestáticas, discos duros o dispositivos de almacenamiento informáticos electromagnéticos, evitando en su caso el uso de bolsas de plástico que puedan causar descargas de electricidad estática y llegar a alterar o destruir los datos latentes sensibles.
- Trasladar los recursos informáticos o *evidencia digital* al lugar de resguardo o de seguridad.

Se recomienda que la o las imágenes forenses de los discos, se realicen a través de un dispositivo duplicador especializado para la captura, en su totalidad, del disco duro origen (espacios libres, no asignados, así como los archivos de intercambio eliminados y ocultos). El dispositivo duplicador deberá cumplir con las siguientes características:

- Debe asegurarse que no alterará el disco duro original.
- Podrá acceder a discos SATA, ATA, SCSI e IDE.
- Deberá verificarse la integridad de la imagen de disco generada.
- Debe bloquear la escritura del disco, para asegurar la inalterabilidad del elemento de almacenamiento accedido.

2. Obtención de la información dinámica o el procesamiento

Anticipadamente a la obtención o generación de imágenes forenses en el lugar adecuado para realizar la investigación en estudio, es conveniente y necesario considerar la obtención o elaboración de los datos en tiempo real, así como de la información dinámica o en el procesamiento. Esta es aquella información que se disipa o pierde al interrumpirse la alimentación eléctrica, es decir, al apagar el recurso informático. Por ello, se deben realizar los subsiguientes pasos:

a) Registrar la fecha, hora del sistema y zona horaria.
b) Determinar quién o quiénes se encuentran con una sesión abierta, ya sean usuarios locales o remotos.
c) Obtener la configuración de red del equipo.
d) Verificar y registrar todas las conexiones activas.
e) Registrar los puertos TCP/UDP abiertos, así como las aplicaciones asociadas a la escucha.
f) Consultar las tablas de ruteo y ARP.
g) Registrar todos los procesos activos.
h) Documentar todas las tareas y comandos efectuados durante la recolección.
i) Examinar y extraer los registros de eventos.
j) Obtener y examinar los archivos de configuración relevantes del sistema operativo.
k) Verificar los registros de eventos de seguridad del sistema, aplicaciones y servicios activos.
l) Configuración de las políticas de auditoría del sistema operativo.

m) Documentar archivos temporales, de correo electrónico y de navegación en internet.
n) Documentar en el registro de cadena de custodia y formato de la entrega-recepción de recursos informáticos o *evidencia digital*.

3. Generación de la evidencia digital forense

Ulteriormente o después de analizado el procedimiento de la revisión de la información dinámica contenida y obtenida, los expertos autorizados deberán de realizar la imagen forense del equipo analizado, atendiendo los siguientes pasos:

a) Apagar el equipo desde el sistema operativo.
b) Desconectar el cable de almacenamiento eléctrico.
c) Retirar las unidades extraíbles.
d) Descargar la propia electricidad estática, mediante pulseras antiestéticas.
e) Desconectar el bus de datos del disco duro (SATA, ATA, SCSI, e IDE).
f) Desconectar el cable de alimentación eléctrica del disco duro.
g) Desconectar el disco duro del chasis del recurso informático, para no dañar el circuito electrónico.
h) Montar el disco duro origen al dispositivo duplicador.
i) Montar el disco duro destino al dispositivo duplicador.
j) Efectuar una o dos copias de la evidencia digital, una para el análisis en el laboratorio de criminalística especializada y personal autorizado, y del original se asegura su embalaje y traslado.
k) Generar una suma de comprobación de la integridad de cada copia, mediante el empleo de funciones *hash*, tales como MD5 o SHA 1.
l) Guardar el resultado generado por las copias duplicadas.
m) Documentar en el registro de cadena de custodia, y acorde al formato de entrega-recepción de los recursos informáticos o *evidencias digitales*.

4. Análisis de la imagen digital forense

Posteriormente de haber obtenido y trasladado la *imagen digital forense,* técnica y metodológicamente se realizará un análisis y estudio completo, metódico, descriptivo y pormenorizado en el lugar especializado designado en tecnologías de la información del conocimiento, por un conjunto de herramientas informático-forenses con la finalidad de poder obtener la siguiente información:

i. Tipo de sistema operativo.
ii. Fecha, hora y zona horaria del sistema operativo.
iii. Versión del sistema operativo.

iv. Número de particiones.
v. Tipo y esquema de particiones.
vi. Listado de todos los nombres de archivos, con fecha y hora.
vii. Registro del espacio asignado.
viii. Recuperación de archivos eliminados.
ix. Búsqueda de archivos ocultos con palabras claves.
x. Listado de todas las aplicaciones existentes en el sistema.
xi. Búsqueda de programas ejecutables sospechosos.
xii. Identificación de extensiones de archivos sospechosos.
xiii. Listado de todos los archivos protegidos con claves.
xiv. Listado del contenido de los archivos de cada usuario en el directorio raíz.
xv. Certificación de los datos a través del algoritmo de *hash* al finalizar la detección, recolección y registro.
xvi. Conservar las copias del software utilizado.

5. Dato de prueba, dictamen, informes de la evidencia digital

Inmediatamente después de realizado el análisis o estudio especializado en Tecnologías de la información de la *evidencia digital* latente, deberá ser utilizado como un *dato de prueba*. Un dato de prueba se define como la referencia al contenido de un determinado medio de convicción aun no desahogado ante el órgano jurisdiccional, que se advierta idóneo y pertinente para poder establecer razonablemente la existencia de un hecho delictivo y la probable participación del imputado. Definidos como *medios* o *elementos de prueba,* son toda fuente de información que permite reconstruir los hechos; específicamente, la *prueba* es todo conocimiento cierto o probable sobre un hecho que, ingresado al proceso en una audiencia y desahogada bajo los principios de inmediación y contradicción, sirve al tribunal de enjuiciamiento como elemento de juicio para llegar a una conclusión cierta sobre los hechos materia de la acusación.[12] La prueba es utilizada preferentemente con la entrega de dos reportes:

A. Informe ejecutivo elemental:

Consiste en el resultado de las investigaciones y análisis especializado efectuado, en el cual deberá utilizarse una terminología no técnica, con un lenguaje común, entendible. Se expondrán los hechos más destacables o importantes de los recursos informáticos o *evidencia digital*, previamente analizados, así como las conclusiones a que se arribaron, con la finalidad de poder orientar al interesado o autoridad solicitante. Debe contener los siguientes puntos:

[12] Benítez Tiburcio Mariana, Código Nacional de Procedimientos Penales Comentado, Gobierno de la Administración Pública, Biblioteca Mexicana del Conocimiento, México, marzo 2015, p. 244.

1) Motivos de la investigación.
2) Desarrollo de la obtención y tratamiento de los recursos informáticos o *evidencias digitales*.
3) Resultado del análisis.
4) Conclusiones.

B. Informe técnico especializado:

Reside específicamente en una exposición detallada, descriptiva y pormenorizada del análisis estructurado y organizado de los recursos o registros informáticos de *evidencias digitales*, que describe en profundidad la técnica y metodologías empleadas y los hallazgos que contenga la información identificada para la utilidad de cada caso. Describen y representan los procedimientos y elementos técnicos utilizados en el estudio y análisis de las evidencias, en el cual se precisan las razones determinantes, que son las síntesis consideradas que permiten fundamentar u orientar las conclusiones de manera clara, firme y congruente, en término de los siguientes puntos:

1) Descripción de la evidencia.
2) Información relevante del sistema analizado.
3) Análisis de la *evidencia digital* documentada.
4) Técnica y metodología utilizada.
5) Descripción de los hallazgos.
6) Conclusiones claras, entendibles, firmes y congruentes.
7) En su caso, identificar al autor o autores de la *evidencia digital*.
8) Nombre y firma del experto en informática de la información que lo elaboró.

Estos apuntamientos de ordenamientos técnicos y metodológicos se aplican en las estrategias jurídicas dentro de la Fiscalía Especializada en Materia de Delincuencia Organizada, junto con el apoyo de elementos adiestrados de la Policía Federal, la Agencia de Investigación Criminal de la Fiscalía General de la República, la Policía Federal Ministerial o la Policía de Investigación, quienes fungen como responsables de las investigaciones. En compañía de peritos profesionales expertos en las ciencias forenses, y principalmente en tecnologías de la información, deberán de robustecerse las líneas de investigaciones en estas ramas del conocimiento. Inclusive con el avance de las ciencias y del conocimiento moderno, increíblemente los delincuentes en las sociedades estatales, nacionales e internacionales, equipados con la utilización de tecnologías de punta, manipulan el conjunto de técnicas, métodos, procesos o *know-how*.

Con el propósito y la finalidad de poder facilitar, procedimentalmente, la búsqueda o la pesquisa de datos de prueba (o descubrimiento probatorio) en las infracciones de criminales en su comisión del delito en materia federal, local o militar —quienes buscan en todo momento, eludir o distorsionar las estrategias a las autoridades

operativas responsables de las indagaciones de crímenes—, en este sentido resulta necesario y fundamental que existan o se implementen constantemente cursos de capacitación o profesionalización especializados en estas materias de la información y comunicación avanzadas (TICs). Hoy en día, se han convertido en herramientas necesarias o fundamentales en el auxilio a la persecución de los delitos y delincuentes, en materia federal, del fuero común y militares. También resultan inescapables estas capacitaciones al personal del Poder Judicial de la Federación, como jueces y magistrados federales, locales y militares, responsables en la administración e impartición de la justicia.

En este sentido, también se requiere una mejor capacitación y profesionalización, en tecnologías de la información y comunicación, a los elementos de policías de la Agencia de Investigación Criminal, así como de Investigación Federal Ministerial, quienes como adiestrados e instruidos operativos conducirán las líneas de investigación en cada uno de los casos; asimismo, para que tengan capacidad de establecer los alcances y aplicabilidades en los *modus operandis* de los grupos delincuenciales en materia federal, local o militar. De igual forma, resulta conveniente profesionalizar y capacitar a los *peritos profesionales especializados* o expertos en las tecnologías de la información y comunicación, quienes suscribirán e informarán los resultados de la preservación, identificación, fijación, embalaje y durante toda la cadena de custodia.[13] Por medio del estudio de las TICs en el laboratorio de criminalística,[14] los peritos pueden identificar las *evidencias digitales* latentes u ocultas en los equipos tecnológicos utilizados en la comisión del delito federal, del fuero común o militar que se investiga.

En esa virtud, es menester inmortalizar a los tratadistas e investigadores como son Hans Gross de Graz[15] (Austria, 9 diciembre 1847-15 diciembre de 1915). Considerado como el padre de la criminalística (que se define como un cúmulo de conocimientos auxiliares del derecho), relató lo siguiente: "el análisis sistemático de las huellas dejadas por el culpable" *(viran)* "la metodología de la investigación del hecho a los datos que aportaban las evidencias físicas, mucho más confiables que el testimonio de testigos". Asimismo, recomienda: "hay que proceder con extraordinaria calma y tranquilidad en el lugar de los hechos, pues sin ella se malograría lastimosamente el éxito de la investigación".

---

13 Vivas Botero, Lugar de los Hechos, define como ***Cadena de Custodia:*** como el procedimiento que consiste en la manipulación adecuada del elemento material de prueba o evidencia física, en procura de conservar su autenticidad y garantizar su inalterabilidad, para lo cual debe hacerse una rigurosa recolección, fijación, embalaje, etiquetado, movimiento, depósito y documentación, partiendo de quien lo encuentra, hasta su disposición final. Editorial Leyer, Colombia, 2006, p. 308.

14 Lorente Acosta, J.A., La ***Evidencia Digital*** latente se está trabajando con equipos informáticos que permiten un estudio y grabación tridimensional de la escena del crimen y su posterior recreación a escala milimétrica.

15 Op. Cit. P. 30.

Para Alphonse Bertillón[16] (22 de abril 1853, París, Francia- 13 de febrero de 1914, Abuené du Trocadéro, París, Francia) fue un policía francés, investigador e impulsor del método de individualización antropológica, quien decía: "Solo se ve lo que se mira, y solo se mira lo que se tiene en la mente". De igual forma, recordando al jurista-español del siglo de oro, Baltazar Gracián y Morales, quien nació en Belmonte, cerca de Calatayud (Zaragoza), el 8 de enero de 1602, y murió en Tirazona, el 6 diciembre de 1658, alguna vez dijo: "lo bueno y lo breve dos veces bueno". Asimismo, en recuerdo imperecedero del doctor Luis Rafael Moreno González[17] de México (nació el 28 noviembre 1931, y falleció el 7 de marzo de 2021); científico, investigador emérito y doctor *honoris causa* del Instituto Nacional de Ciencias Penales, así como miembro de número de la Academia Mexicana de Ciencias Penales, decía: "las primeras horas de la investigación son inapreciables y, en estas cosas, el tiempo que pasa representa la verdad que huye"; así como: "no hay malhechor que no deje detrás de sí alguna huella aprovechable".

Todos aquellos autores citados fueron ilustres y gloriosos humanistas, quienes siempre con su ciencia y su saber en la criminalística científica, consideraron que la ausencia de herramientas y tecnologías modernas, especializadas y prácticas en resolver las cuestiones criminales (las cuales se apliquen, empleen y utilicen con conocimientos técnicos-científicos para poder resolver las cuestiones criminales), es una cuestión que sigue al hombre, como la sombra sigue al cuerpo.

16 Op. Cit. P. 32

17 Moreno González, Luis Rafael, *El lugar de los hechos y la policía especializada*, Instituto de Investigaciones Jurídicas, UNAM, México, 2015.