LA AUDITORÍA FORENSE COMO FUNDAMENTO METODOLÓGICO EN LA DETECCIÓN DE CASOS DE FRAUDES INFORMÁTICOS

Esp. Gerardo Asdrúbal Díaz Varela
Universidad Latinoamericana y del Caribe (ULAC)
gerardo.diazv@gmail.com
Venezuela
Orcid ID

Recepción: 12 de diciembre del 2020. Aceptación: 11 de enero del 2021.
Innovación tecnológica como proceso

Resumen

Las organizaciones se sirven de la auditoria forense para mitigar los riesgos asociados al fraude, optimizando igualmente su sistema de control interno; esta auditoria se constituye en herramienta incuestionable de lucha contra el fraude, contribuyendo positivamente en su prevención y detección; el objeto de esta investigación, es caracterizar la importancia de la auditoria forense como fundamento metodológico en la detección de casos de fraude informático; bajo esta concepción se valoran técnicas y procedimientos de auditoria, el análisis forense informático, así como el fundamento jurídico que le asiste, aspectos que en suma fortalecen la metodología aplicada y sus resultados. Esta investigación corresponde a un estudio documental, de nivel descriptivo y diseño bibliográfico; expone, como la auditoría forense emerge como acción gerencial, de prevención y detección, que a través de la aplicación de las mejores prácticas de esta disciplina, conlleva a mitigar y procesar aquellas causas tipificadas como fraude informático.

Palabras clave: Auditoria forense; fraude informático; derecho probatorio; evidencia y prueba digital.

FORENSIC AUDITING AS A METHODOLOGICAL FOUNDATION IN THE DETECTION OF CASES OF COMPUTER FRAUD

Abstract

Organizations use forensic auditing to mitigate the risks associated with fraud, optimizing their internal control systems; this auditing method is an unquestionable tool in the fight against fraud, contributing positively to its prevention and detection. The purpose of this investigation is to characterize the importance of forensic auditing as a methodological foundation in the detection of cases of computer fraud; under this conception, auditing techniques and procedures, computer forensic analysis, as well as the legal basis that assists it are evaluated, aspects that in sum strengthen the applied methodology and its results. This research corresponds to a documentary study, at a descriptive level and bibliographic design;

L'AUDIT MÉDICO-LÉGAL COMME FONDEMENT MÉTHODOLOGIQUE DANS LA DÉTECTION DES CAS DE FRAUDE INFORMATIQUE

Résumé

Les organisations utilisent l'audit médico-légal pour atténuer les risques associés à la fraude, en optimisant également leur système de contrôle interne; Cet audit constitue un outil incontestable dans la lutte contre la fraude, contribuant positivement à sa prévention et à sa détection; Le but de cette enquête est de caractériser l'importance de l'audit médico-légal en tant que fondement méthodologique dans la détection des cas de fraude informatique; Selon cette conception, les techniques et procédures d'audit, l'analyse médico-légale informatique ainsi que la base juridique qui l'assiste sont évaluées, aspects qui en somme renforcent la méthodologie appliquée et ses résultats. Cette recherche

it exposes how forensic auditing emerges as a management, prevention, and detection action, which, by applying the best practices of this discipline, leads to mitigating and processing those causes classified as computer fraud.

Keywords: Forensic auditing; computer fraud; evidentiary law; evidence and digital proof.

correspond à une étude documentaire, un niveau descriptif et une conception bibliographique; Il expose comment l'audit médico-légal apparaît comme une action de gestion, de prévention et de détection, qui, grâce à l'application des meilleures pratiques de cette discipline, conduit à atténuer et à traiter les causes classées comme fraude informatique.

Mots-clés: Audit médico-légal; fraude informatique; droit de la preuve; preuves et preuves numériques.

Introducción

Las tecnologías de la información irrumpen de manera constante en la sociedad global, favoreciendo la actividad comercial y de producción, transformando la dinámica financiera y con ello el flujo de capitales; sin embargo, este crecimiento vertiginoso impulsado por estas tecnologías, ha venido acompañado de novedosas formas delincuenciales. Las tecnologías de la información (TI) se constituyen hoy día, como el aliado más importante organizacionalmente hablando, pues su influencia en los negocios globales y en la sociedad en general no está en discusión, su avance tributa beneficios a personas y organizaciones, potenciando sus capacidades.

Esta interacción virtual adopta complejos esquemas de seguridad, que le brindan a los usuarios una relativa protección, pues el riesgo inherente al usos de las tecnologías siempre estará presente, razón por la cual se invierten recursos importantes a los fines de mitigar las amenazas, que en forma de intentos de fraude subyacen bajo la figura del delito informático. Considerando la complejidad de este tipo de delito, la auditoría forense se conforma como la disciplina que revelará, mediante el uso de metodologías, técnicas y herramientas, los elementos que se articulan para la ocurrencia de este tipo de fraude.

La auditoría forense, para evaluar los procesos de la organización desde el punto de vista investigativo, incorpora en su desarrollo múltiples tareas, que van como lo señala Márquez (2018), desde la identificación del evento, el análisis de los hallazgos y la recolección de evidencias, la determinación de la prueba para luego de cumplido estos protocolos, presentar el informe de resultados; ahora bien, disponer de metodologías e insumos que intensifiquen la investigación, sin comprometer la necesaria dinámica relacionada con el desarrollo de las actividades de auditoria, que mitiguen la presencia de errores durante el proceso de ejecución, al tiempo que proveen un marco de trabajo diligente y ordenado, que consecuentemente favorecerá la conformación y obtención de evidencias que serán presentadas como prueba en un proceso judicial, representa un trabajo arduo y complejo.

Los delitos informáticos, señalan Acosta, Benavides y García (2020), destacan por sus características convergentes que acentúan diversos tipos de acciones ilegales, de allí la complejidad que representa demostrarlos en un juicio, toda vez que la tarea de investigar a un delincuente informático incorpora actividades con alto nivel de especificidad y depuración, que el exigido por un delito común; a ello debe incorporarse la habilidad, velocidad e inmediatez con la que éstos transgresores actúan, así como la constante evolución, adaptación y expansión de estas prácticas delictivas.

Uno de los elementos que permite exponer y soportar el delito informático, está representada por la evidencia digital; considerando lo expuesto por Aguilar (2019), las evidencias digitales, son elementos físicos aunque de carácter intangible, pues suelen ser rastros o acciones que quedan registradas en un equipo informático, y que permiten comprobar la participación o realización de algún tipo de acción por parte de un usuario o intruso, que emplea un sistema informático determinado; conformándose dicha traza en una especie de huella digital-informática de los ciberdelincuentes.

En este orden, se observa que las TI se constituyen en un instrumento procesal de gran utilidad al brindar los elementos que permiten obtener la prueba digital, por tanto los especialistas en derecho, las áreas de seguridad integral y gestión humana, así como todo el entorno gerencial y empresarial emplean este insumo como pieza fundamental del entramado de control.

Ahora bien, el proceso de auditoria forense y el análisis de la data informática, indica Nigrini (2020), suelen presentar algún tipo de limitaciones, no obstante es condición y parte del protocolo de investigación la aplicación de pruebas enfocadas en el uso de una variedad de métodos cuantitativos, incluida la Ley de Benford, la detección de valores atípicos, la detección de duplicados, comparación con puntos de referencia, métodos de series de tiempo, puntuación de riesgo y, a veces, simplemente lógica estadística; los objetivos de las pruebas son producir una pequeña muestra de transacciones sospechosas, un pequeño conjunto de grupos de transacciones o una puntuación de riesgo relacionada con transacciones individuales o un grupo de elementos; sin embargo, se deben extremar las pruebas analíticas, a objeto de detectar en el proceso de reconstrucción de las evidencias digitales, que estás no hayan sido modificadas

Volumen 06 - N° 02, Julio - Diciembre 2021
Depósito Legal N° DC2017000305/ISSN: 2542-3142

deliberadamente por los propios infractores, que puedan haber sufrido deterioro, o peor aún, que hayan sido suprimidas, por lo que es necesario contar con herramientas tecnológicas, amén de una metodología particular, que permita la recuperación de datos, aspecto este, que reviste vital importancia ya que normalmente son las pruebas principales que se pueden presentar cuando se determina la ocurrencia de un delito informático.

Por su parte, los archivos, documentos y demás insumos de carácter digital que se derivan de la auditoria forense y el análisis informático asociado, se constituyen en evidencias de este tipo de delito, por cuanto develan datos importantes que permiten establecer tanto su existencia como las responsabilidades inherentes; de allí la importancia que los órganos de investigación designados, colecten, custodien, resguarden y examinen estas evidencias con extrema rigurosidad, a objeto que las mismas no sufran ningún tipo de cambios o transformaciones, deterioro, destrucción, desaparición o substracción.

En este sentido, los auditores forenses involucrados en la investigación de delitos informáticos tal como lo señala Nigrini (2020), desarrollan su actividad en la detección de hallazgos y trazas de tipo digital, cuyas características más resaltantes son su volatilidad, inestabilidad y su breve permanencia; considerando estos elementos, el análisis forense informático que aplica este tipo de auditoria reviste formalidades y protocolos que son desarrollados en cada una de las fases de ejecución, e incorporados a su metodología; estas acciones en conjunto se conforman en instrumentos que permiten asegurar la oportunidad y veracidad de los resultados.

Por lo señalado anteriormente, el propósito de esta investigación es exponer la importancia de la auditoria forense como fundamento metodológico en la detección de casos de fraude informático al tiempo que se constituya como practica imprescindible en la detección del fraude informático.

Del planteamiento formulado anteriormente, se derivan las siguientes interrogantes:

- ¿Cuál es la importancia de la auditoria forense como fundamento metodológico en la detección de casos de fraude informático?

- ¿Cómo la auditoria forense se conforma en herramienta para la detección de elementos asociados al fraude informático?

- ¿Qué elementos se configuran en auditoria forense que se relacionen con los principios de derecho probatorio para los casos de fraude informático?

- ¿Qué oportunidades de mejora en la metodología que desarrolla la auditoria forense se pueden identificar, que coadyuven al cumplimiento del alcance definido para los casos de fraude informático?

Considerando estas interrogantes, el objetivo general de la presente investigación se dirige a exponer la importancia de la auditoria forense como fundamento metodológico en la detección de casos de fraude informático; en este orden los objetivos específicos que permitirán el desarrollo del objetivo general, conlleva en primer término a determinar los aspectos que configuran a la auditoria forense como herramienta en la detección en los casos de fraude informático; en segundo lugar, describir los principios generales del derecho probatorio y su relación con la auditoria forense para los casos de fraude informático; y finalmente identificar oportunidades de mejora en los procedimientos de auditoria forense dirigidos a los casos de fraude informático.

Justificación

Al conformarse características de intangibilidad y volatilidad, en los resultados obtenidos del análisis forense informático, presentes en la metodología de la auditoria forense, puede conllevar a considerarlas como información de carácter parcial, por cuanto solo una de las partes la posee y que generalmente es quién las presenta a la instancia legal como prueba de sus demandas, por lo que su cuestionamiento siempre estará presente. Esta predisposición, permite que cualquier demanda o causa se encuentre con un problema adicional, como lo es, presentar medios de prueba basados en evidencias digitales pues su admisión, práctica y valoración, conlleva un reto para ambas partes.

La presente investigación favorecerá el análisis técnico y jurídico, que dirige la auditoria

Volumen 06 - N° 02, Julio - Diciembre 2021
Depósito Legal N° DC2017000305/ISSN: 2542-3142

forense a los elementos inmersos en el fraude informático; destaca igualmente el valor que genera el cumplimiento de los protocolos que exige el análisis forense, y el beneficio de incorporar valor agregado a la metodología empleada en su manejo, a través de las buenas prácticas que aplican para esta disciplina.

Asimismo, la investigación destacará el principio de legalidad y el consecuente valor probatorio de la evidencia digital resultante de la auditoria forense, aspecto que confirmará su calidad, veracidad, oportunidad y pertinencia, como medio para garantizar la aplicación de justicia.

La investigación se limitará al análisis de los procesos metodológicos y mejores prácticas aplicadas en el desarrollo de una auditoria forense para la detección de casos de fraude informático.

Visión del entorno

Auditoría forense

La auditoría forense se presenta como una disciplina que dirige su actividad, como lo señala Márquez (2018), a la investigación y obtención de pruebas sobre la existencia de delitos relacionados con los activos organizacionales o que comprometan la operatividad informática, es así como la auditoria forense contribuye con su aporte experto a quienes administran justicia. En el ejercicio de la auditoría forense se analiza los procesos de la organización, evaluando criterios, excepciones, eventos financieros, procesos operativos e informáticos, riesgos, activos y patrones de conducta que pueden ser considerados irregulares; esta actividad es llevada a cabo a través de un análisis sistemático que incluye la data física y lógica, procurando la obtención de pruebas legales de hechos presuntamente delictivos que podría perjudicar y/o comprometer intereses de carácter público o privado.

La auditoría forense, busca la razonabilidad de las cifras de tipo financiero, la sinceridad y no repudio de la data que opera y reposa en los sistemas de información gerencial, es así, refiere Martínez (2020) como debe profundizar en la adecuada revisión de las cifras,

registros, operaciones y transacciones de tipo contable, operativo e informático, verificando la lógica de dichas operaciones y que efectivamente correspondan a la realidad económica de la organización; ahora bien, esta tarea implica un profundo análisis y un trabajo metódico y organizado que conlleva una inversión significativa en horas-hombre, pues la tarea delicada y responsable en la búsqueda de hallazgos de auditoría que se puedan transformar en prueba judicial, así lo amerita.

Siguiendo este orden, la auditoría forense establece una diferencia bien marcada con otras perspectivas de control en su función de carácter preventivo, pues de acuerdo a lo señalado por Márquez (2018) su operatividad se sustenta en un programa de aseguramiento constante dirigido al riesgo de fraude, para lo cual exhorta a la gerencia a aplicar una serie de medidas de control, que incluye entre otros la creación e implementación de prácticas y programas antifraude, mecanismos de alerta temprana, así como sistemas de gestión de denuncias; de esta manera, se establecen esquemas de detección de fraudes que deben ser investigados en profundidad y llevados a las instancias legales que correspondan; la auditoria forense considera el fraude como un subterfugio con intencionalidad para la ocurrencia irregular de incidentes de carácter financiero, operativo, informático o de aquellos relativos a la apropiación indebida de activos de naturaleza material.

La evaluación del SCI a través de los mecanismos de aseguramiento, análisis de riesgo y detección de fraude previamente citados, permitirá como lo indica Martínez (2020), identificar a los posibles responsables de operaciones fraudulentas, los presuntos involucrados que pudiesen formar parte de la misma organización o con terceros relacionados, así como su modo de operar; ahora bien, los resultados que se generen de dicha evaluación, indicaran el camino en el diseño de los procedimientos de auditoría que ofrezcan certeza razonable para la detección de distorsiones producidas por fraude o error y, cuyo efecto material afecte las operaciones de la organización, siendo estos los elementos primordiales que servirán de base para la planificación de la auditoría forense; en este contexto, las características y naturaleza de los activos, las personas o los procesos que se van a auditar son elementos a considerarse durante la planificación; en este orden la capacidad y experiencia del auditor es de principal

Volumen 06 - N° 02, Julio - Diciembre 2021
Depósito Legal N° DC2017000305/ISSN: 2542-3142

relevancia, dado que por la naturaleza del trabajo, se requiere del juicio profesional durante todo el proceso; aspectos que representan un gran respaldo, pues esta experticia facilitara la toma de decisiones relacionadas con la metodología que se aplique, con el alcance, los costos y la ética, entre otros aspectos de importancia.

Considerando lo ya expuesto, los procedimientos de auditoria forense se adecuaran en función de la naturaleza del delito a investigar, no obstante el desarrollo de su actividad debe responder a las siguientes tareas: planificación, evaluación de riesgos y análisis preliminar, recolección y análisis de evidencias, revisión y análisis documental (física e intangible), elaboración y presentación del informe de resultados, plan de acción correctiva y cierre; en la figura Nº 1, donde se detalla básicamente el orden y/o pasos que deben seguirse en la oportunidad de abordar un trabajo de auditoria forense que incorpore procesos de análisis forense informático cuyo eje transversal lo constituye la evidencia digital.

Figura 1. Procesos de la Auditoría Forense y el análisis forense informático
Fuente: Elaboración propia (2020) apoyado en datos de Martínez (2020)

Bajo esta premisa, la auditoría forense se establece como elemento científico en la reconstrucción de hechos relacionados con conductas ilegales dirigidos a los entornos informáticos, financieros, de investigación de fraudes, de cálculos de daños económicos, así como en herramienta de análisis prospectivo en las diferentes disciplinas que le asisten.

Fraude informático

El desarrollo tecnológico y en particular el relacionado con la información y comunicación irrumpen en el quehacer cotidiano, tanto que, lo que en un tiempo se consideraba un suceso extraordinario, hoy día es algo habitual, pues estas TI no operan exclusivamente en las organizaciones o se conforman como privilegios de determinadas profesiones, sino que su transcendencia incorpora a la sociedad en general; ahora bien, estos medios que representan un gran avance en el desarrollo del comercio y los negocios globales, es empleado igualmente en la comisión de delitos, eventos que como refiere Devia (2017) se transforman en un fenómeno de creciente riesgo y perjuicio, cuya tipificación y judicialización penal en algunos casos pudiesen considerarse como insuficientes.

En este contexto y previo a caracterizar el fraude informático, es necesario abordar su conceptualización y los elementos que se asocian al fraude en términos generales; en este orden, el fraude representa un delito de engaño, una violación a la confianza, por tanto, es eminentemente deliberado e intencional, las categorías de fraude van desde el timo común o individual, hasta la evasión de impuesto, estafa empresarial, delitos de cuello blanco, fraude ocupacional, evolucionando con las tecnologías disruptivas actuales, hasta encontrarnos con nuevas modalidades de fraude informático, que no detienen su avance.

En términos generales el fraude informático comprenden conductas que se valen de medios informáticos para quebrantar intereses jurídicamente protegidos como el relativo a la intimidad, al patrimonio económico, a la seguridad, entre otros, así como conductas atentan directamente a herramientas y aplicaciones informáticas, incluidos equipos de cómputo y servidores, ahora bien, cuando la conducta lesiona distintos intereses jurídicos protegidos, refiere Devia (2017), la forma en que se comete este delito es muy amplia y al momento de emplear un equipo de

Volumen 06 - N° 02, Julio - Diciembre 2021
Depósito Legal N° DC2017000305/ISSN: 2542-3142

computación como instrumento delictivo, existe la posibilidad de usar la analogía a objeto de adaptar la figura penal a los avances de la informática. Bajo esta visión, los procedimientos de auditoría forense son más específicos y deben estar orientados a detectar posibles errores de significada importancia; en este sentido, los procedimientos de auditoría deben alinearse con los riesgos de fraude y las evaluaciones de riesgo de fraude.

Según el teórico y criminólogo Donald Cressey, en su propuesta del triángulo de fraude (Cressey-1961), destacó que hay tres elementos interrelacionados que permiten a alguien cometer fraude: el motivo que impulsa a una persona a querer cometer el fraude, la oportunidad que le permite cometer el fraude y la capacidad de racionalizar el comportamiento fraudulento; la vulnerabilidad presente en una organización para aquellos capaces de superar los tres elementos del triángulo de fraude es el riesgo de fraude; este riesgo puede originarse de fuentes internas y externas a la organización.

En concordancia con lo planteado, los defraudadores dejan ver en su perfil, una serie de competencias atractivas para cualquier empleador, no obstante, orientan estas capacidades a sus motivaciones particulares y contrarias a los intereses de las organizaciones y la sociedad en general, mantienen características en común, como su adaptabilidad e innovación, su creatividad y capacidad intelectual.

En este contexto, se observa que el fraude se encuentra en constante innovación, pues entre otras condiciones, cumple el modelo de instrucción a través del ensayo y error e incorpora diversos tipos de modus operandi que son revisados, interpretados, modificados y mejorados por aquellos individuos que irrumpen como una nueva avanzada de defraudadores. Las tendencias tecnológicas se conforman como una barrera de entrada alta para la incursión e incremento del delito de fraude, no obstante, como lo refiere Casey (2019), hay condiciones que se mantiene y mantendrán por mucho tiempo constantes, que no son otras que las relativas a las motivaciones y, a las emociones humanas.

En el marco de la tipificación de esta clase de delito, las características propias de esta transgresión, señala Posada (2017), poseen elementos de especialización y complejidad que la

diferencia de los delitos comunes, toda vez que engloba, entre otras, la irrupción de tecnologías como las TI, que requiere para su abordaje además de competencia y formación profesional específica, el uso de técnicas y herramientas especializadas de protección, unas tangibles (hardware) otras intangibles (software), pero también, porque los comportamientos subyacentes reflejan una muy compleja evolución y transformación de sus componentes, particularmente los que conllevan a la acción y sus resultados, todo ello dentro del contexto delincuencial que irrumpe con irreverencia; lo que implica una adaptación y/o evolución de las doctrinas jurídicas acorde a las exigencia que impone el entorno tecnológico.

Evidencia digital

El análisis de la escena del crimen y la consecuente colección de evidencias son términos, como lo señala Chisum and Turvey (2017), que se refieren al reconocimiento, documentación, preservación, recolección y transporte de evidencia física y digital para su examen y prueba. Hay diferentes tipos de escenas del crimen y diferentes niveles de procesamiento, cada uno con sus propias limitaciones y consideraciones. Estos esfuerzos deben ser consistentes, integrales y objetivos para proporcionar un registro científico que pueda ser cuestionado por el desarrollo del caso y las preguntas que surjan mucho después que se formalice la escena del crimen. El análisis de la escena del crimen no es competencia exclusiva de los investigadores policiales con conocimientos especiales; sino una responsabilidad que requiere transparencia para proporcionar una base confiable para todos los esfuerzos futuros de reconstrucción y análisis del crimen

La evidencia digital se define, de acuerdo a lo expuesto por Chisum and Turvey (2017), como cualquier dato almacenado o transmitido usando una computadora que respalda o refuta una teoría de cómo ocurrió un delito o que aborda elementos críticos del delito, como la intención o la coartada; los datos referidos en esta definición son esencialmente una combinación de números que representan información de varios tipos, incluidos texto, imágenes, audio y video.

Asimismo, Acurio (2016), expone que la evidencia se conforma por cualquier información o dato, que puede ser empleado para establecer o demostrar la sinceridad y/o veracidad, relativo

Volumen 06 - N° 02, Julio - Diciembre 2021
Depósito Legal N° DC2017000305/ISSN: 2542-3142

a la ocurrencia de un hecho o evento, en términos prácticos, no es otra cosa que, información extraída de un testimonio personal, un documento o un objeto material, utilizada para establecer hechos en una investigación legal o admisible como testimonio en un tribunal de justicia.

Por consiguiente, la evidencia digital es conceptualmente similar a cualquier otra evidencia: es información que impulsa y perfila la ubicación de individuos y eventos con analogía en tiempo y espacio, análisis que permite establecer la relación de causalidad con la ocurrencia de incidentes de carácter delictivo. La evidencia digital como una forma de evidencia física, refiere Casey (2011) crea varios desafíos para los auditores forenses particularmente el dirigido al análisis forense digital; es importante tener en cuenta que es una forma de evidencia desorganizada y compleja que puede ser muy difícil de manejar, si consideramos la información contenida un disco duro, la misma está compuesta por un conjunto desordenado de datos: piezas o porciones de información mezcladas y superpuestas a lo largo del tiempo, solo una pequeña parte de este conjunto datos puede ser relevante para un caso, por lo que es necesario extraer piezas de información útil, unirlas y traducirlas a una forma que pueda interpretarse.

Igualmente, la evidencia digital es generalmente una abstracción de algún objeto o evento digital, un ejemplo de ello corresponde a la instrucción generada por un usuario a una computadora para que realice una tarea específica como enviar un correo electrónico, las actividades resultantes generan trazas de datos que dan solo una visión parcial de lo que ocurrió, solo ciertos resultados de la actividad, como el mensaje de correo electrónico y los registros del servidor, permanecen disponibles para darnos una vista parcial de lo que ocurrió. Además, el uso de una herramienta forense para recuperar un archivo eliminado de un medio de almacenamiento implica varias capas de abstracción desde los campos magnéticos en el disco hasta las letras y números que vemos en pantalla.

Esta evidencia digital o electrónica como también se le conoce, corresponde como lo señala Casey (2019), a información o data almacenada y/o transmitida en formato digital y cuyo contenido total o parcial, posee los atributos necesarios para ser presentada en un juicio; previo a la aceptación de la prueba digital, el administrador de justicia comprobará si esta es pertinente, auténtica, si es creada o forjada, si es relevante, si es necesaria la presentación del original o una copia es suficiente.

En el ámbito digital, nos movemos hacia un espacio más virtual y menos tangible; el intercambio de evidencia digital a menudo implica una copia de los datos que se transfieren, dejando el original esencialmente sin cambios. A pesar de estos detalles, los intercambios de evidencia en el ámbito digital dejan rastros categorizados e individuales que coadyuvan a responder interrogantes críticas o incluso resolver un caso.

Se plantea entonces, una contextualización de la evidencia, dentro del proceso de auditoría, la cual se enmarca dentro del sistema de control interno organizacional; de allí parte su caracterización, destacando entre otras sus particularidades que se encuentran regidas por protocolos y estándares específicos, que la diferencian de la evidencia habitual. Ahora bien, conocer el valor probatorio que se le confiere a las evidencias o pruebas digitales en un litigio, es transcendental, pues la iteratividad que reflejan las tecnologías de la información se traduce en inmediatez, ubicuidad e intangibilidad, al extremo de considerar que los documentos, evidencias y/o pruebas de elaboración digital han reemplazado a los documentos, evidencias y pruebas tradicionales (tangibles).

La evidencia digital puede revelar comunicaciones entre sospechosos y víctima, actividades en línea en momentos clave, e información adicional que proporciona una dimensión digital a la investigación. En las intrusiones informáticas, señala Casey (2019), los atacantes dejan múltiples rastros de su presencia en todo el entorno, incluidos los sistemas de archivos, los registros del sistema y los registros a nivel de red; además, los atacantes incluso, podrían transferir elementos de la escena del crimen con ellos, como contraseñas de usuario robadas o datos sensibles, en un archivo, base de datos e incluso en la nube; dicha evidencia puede ser útil para vincular a un individuo con una intrusión.

En este sentido, los datos digitales, refiere Casey (2011), se encuentran en nuestro alrededor y deben extraerse de forma rutinaria para cualquier tipo investigación; es probable que alguien que se encuentre involucrado en un delito, opere un equipo de computación, use un dispositivo móvil o acceda a Internet; por tanto, toda investigación de carácter corporativo o institucional debe considerar esta información como relevante, incluidas aquellas que se encuentren dispuestas y/o almacenadas en los sistemas y aplicaciones informáticas usadas

Volumen 06 - N° 02, Julio - Diciembre 2021
Depósito Legal N° DC2017000305/ISSN: 2542-3142

por sus empleados, estén estos ubicados en su espacio laboral o en su domicilio particular.

Ahora bien, si consideramos el principio de intercambio de Locard, tal como lo refiere Casey (2011), el contacto entre dos elementos dará lugar a un intercambio; este principio se aplica a cualquier contacto en la escena del crimen, incluso entre el delincuente y la víctima, entre una persona con un arma y entre las personas y la propia escena del crimen. En resumen, siempre habrá evidencia de la interacción, aunque en algunos casos puede que no se detecte fácilmente; esta transferencia ocurre tanto en el ámbito físico como en el digital y puede proporcionar vínculos entre ellos como se muestra en la Figura 2. El vínculo entre el delincuente y la escena del crimen se vuelve más fuerte y más fácil de demostrar.

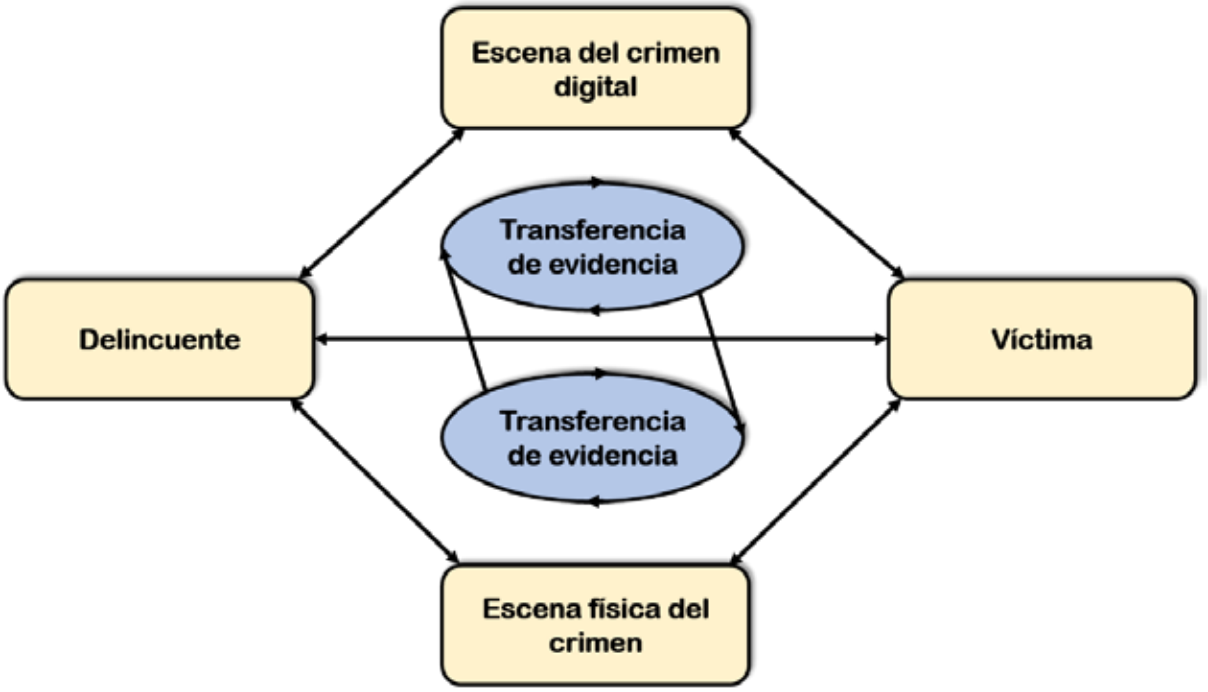

Figura 2. La transferencia de pruebas del Modelo de Locard en las dimensiones física y digital.
Fuente: Adaptación del autor (2020) del presentado por Casey (2011)

Ahora bien, la evidencia digital puede revelar cómo se cometió un delito, proporcionar pistas de investigación, refutar o respaldar declaraciones de testigos e identificar posibles sospechosos. En este orden, la auditoria forense como metodología para la detección de fraudes informáticos, combina elementos del derecho y la informática para recopilar y analizar datos de

sistemas digitales, redes, comunicaciones inalámbricas y dispositivos de almacenamiento de una manera que sean admisibles como prueba en un tribunal de justicia.

Derecho probatorio

Las tecnologías de la información (TI), se sirven de los múltiples insumos en hardware y software que dispone para facilitar y dar fluidez a los múltiples procesos que desarrollan las organizaciones en sus plataformas de negocios; los medios informáticos que incorporan las TI provee, como señala Mayer y Oliver (2020) de instrumentos, material y métodos para almacenar, procesar, transmitir, información y datos en formato digital, a través de equipos y sistemas de información. La integración de la auditoría forense y el análisis informático actúan como una sola red, se sirven de las TI a través del empleo de metodologías de evaluación, así como de hardware y software especializado bajo una visión investigativa y de derecho, aspectos que posibilitan el tratamiento, análisis, almacenaje y recuperación de información, mediante técnicas adecuadas, que tributan al campo forense y jurídico.

Al abordar un proceso investigativo donde lo informático y lo forense se conforman como el eje transversal que soportara los resultados de los hallazgos, se deben generar tal como lo plantea Nelson, Phillips and Steuart (2019), metodologías que garanticen la transparencia y credibilidad, es decir que revelen de manera clara y precisa la realidad de los hechos, transformando este proceso investigativo en una herramienta imprescindible tanto para el desarrollo de planes de acción correctiva, como para la determinación de responsabilidades y el ejercicio del derecho en el consecuente procedimiento penal, siendo indispensable la obtención de evidencias y su formación como medio de prueba, todo ello a tenor de lo dispuesto en la legislación que regulen su presentación y tratamiento procesal.

De ahí, que en aplicación a estos fundamentos, la prueba adquiere una significativa relevancia jurídica, y se constituye en el soporte del proceso judicial, toda vez que los hechos debatidos dentro del mismo, se incorporan, interpretan y aclaran, por medio de los principios probatorios que apliquen; por tanto, estos principios permitirán a quienes procuran como objetivo principal, obtener la verdad de los hechos o al menos alcanzar una cercanía estrecha con la exactitud de la realidad.

Volumen 06 - N° 02, Julio - Diciembre 2021
Depósito Legal N° DC2017000305/ISSN: 2542-3142

Ahora bien, ya evidenciados estos aspectos fundamentales en el ámbito del ejercicio del derecho, se puede afirmar que la prueba se considera como la pieza más importante dentro del engranaje jurídico, de allí deriva su principal característica dirigida al halo de confiabilidad que le rodea y, que permite conducir indudablemente a la revelación y realidad de los hechos; estas acciones en conjunto conllevan a garantizar la objetividad en los fallos judiciales, evitando y/o mitigando los comportamientos arbitrarios que pudiesen presentarse tanto en el transcurso del proceso judicial, como en la decisiones que se incorporan al cierre del juicio; en este contexto, la prueba, como refiere Aguilar (2019), en su admisión y consideración, procede básicamente de datos probatorios legalmente incorporados al proceso, cuya conformación y contenido integren elementos de convicción irrefutables, que finalmente resulten en una decisión judicial ajustada a derecho.

La prueba en entornos informáticos

En el transcurrir de la tercera y cuarta revolución industrial, los entornos informáticos forman parte esencial de estos procesos de desarrollo y evolución, y se integran en un sinnúmero de actividades del quehacer humano; por tanto, se producen millones de transacciones por minuto, que generan un gran volumen de datos y documentos electrónicos que abarca la globalidad de la economía, incluida las transacciones de carácter personal, empleando como medio de transmisión y comunicación la dinámica y fluidez que suministra el ciberespacio.

En este orden, la sociedad se ha servido de los medios y soportes digitales, para garantizar un nuevo medio de prueba que guarde relación con el tradicional, pero en cuanto a su conformación, esta debe estar sujeta a cuidadosos procesos que mantengan y garanticen su integridad, estos elementos no convencionales permiten enriquecer el proceso probatorio, conformándose en avances significativos en el ámbito del derecho.

Visto lo anterior, los documentos electrónicos, poseen características excepcionales que revisten un tratamiento particular si lo comparamos con el documento físico y/o convencional; las rasgos distintivos de estos tipos de documentos emergen producto de la interacción y uso masivo de diversas tecnologías disruptivas, como las TIC, las telecomunicaciones y el

comercio y gobierno electrónico, fenómenos propios de la globalización que conlleva a, que diversos países desarrollen legislaciones dirigidas al uso de estas tecnologías, que incorporan entre otras, normas de protección de datos, seguridad de la información, derecho al olvido, extendiendo a través de acuerdos internacionales, dictaminar y fijar parámetros probatorios dirigidos a las trazas y documentos de carácter digital que se generan, considerando siempre los principios de valoración adecuados a este medio tecnológico de prueba.

Dada la acelerada evolución tecnológica y el uso masivo de distintos instrumentos electrónicos, las fuentes de prueba cuyo origen se fundamenta en lo digital, se incrementan de manera exponencial, hallándose en novedosas herramientas informáticas, en equipos e insumos multimedia y/o de comunicaciones, así como novísimos formatos y soportes; no obstante, esta diversidad de fuentes probatorias, se abren camino a través de alguno de los medios de prueba formalmente establecidos; bien como prueba de carácter documental y digital, como prueba derivada de un proceso de peritaje, o a través del reconocimiento judicial; de igual manera, como prueba testimonial o de interrogatorio de las partes y/o del acusado en el proceso penal, mediante el testimonio de la persona o personas que hayan tenido relación y contacto con la herramienta, medio o insumo electrónico.

Los datos o información digital obtenidas de las distintas fuentes de prueba, pueden ser presentados en juicio a través de diferentes medios probatorios, siendo una de ellas el documento digital, es decir, la información es recogida en un soporte electrónico incorporado en un formato determinado que facilite su identificación, al tiempo que permita dársele un tratamiento diferenciado. Ahora bien, la forma material de incorporación al proceso, es el propio documento (información o datos). De esta forma, lo que materialmente se incorpora es el propio soporte en el que se incluye: un pendrive, un disco compacto u otros medios que permitan el almacenamiento de datos; es necesario tener presente que mientras los documentos en soporte físico (papel) pueden ser leídos de forma inmediata, los documentos electrónicos solamente pueden ser objeto de lectura a través de un medio técnico destinado al efecto.

Volumen 06 - N° 02, Julio - Diciembre 2021
Depósito Legal N° DC2017000305/ISSN: 2542-3142

Materiales y métodos

La presente investigación, considerando la fuente originaria de información, es una investigación de carácter documental, toda vez, que la misma se nutre de los estudios e investigaciones ya realizadas, consolidando los diversos criterios que se manejan en el derecho y la informática, y que son relativos a la auditoria forense.

Por consiguiente, la investigación realizada corresponde a un estudio no experimental de tipo documental, la misma se sustenta en los estudios e investigaciones ya realizados en auditoria de sistemas de información, auditoria forense y análisis forense informático, fortaleciendo en consecuencia, los diversos criterios de pertinencia, exhaustividad y actualidad que se manejan en estas disciplinas, y que son relativos a la gestión gerencial.

En este contexto, para la recolección, selección y análisis de documentos se formularon y aplicaron criterios para evaluar la información y sus fuentes, por tanto, su análisis cumplió con criterios de exactitud, pertinencia y relevancia, objetividad, alcance, exhaustividad y actualidad, actividad que permitió la obtención de resultados coherentes de su estudio e interpretación, aspectos que conllevo al investigador a determinar la asociación entre la auditoria forense, la informática forense y la gestión gerencial.

La metodología desarrollada, se ejecutó a través de la revisión bibliográfica que incluyo un mapeo conceptual, definiéndose igualmente el alcance de la revisión y aplicándose un proceso estructurado de búsqueda y análisis; para su transcripción, se empleó una matriz de registro de datos, donde se caracterizaron los autores por tema y relevancia de los aportes, así como su relación con el tema objeto de investigación, tipo de documento analizado (libro, articulo, tesis, trabajo especial de grado, revista), medio de acceso (físico, digital), fecha de publicación, idioma y páginas de ubicación de los aportes para su localización expedita.

El nivel de estudio, de acuerdo con los objetivos planteados en la presente investigación, es del tipo descriptivo, por cuanto se buscó señalar sistemáticamente las relaciones de asociación que se presentan entre aspectos básicos de auditoria, fraude digital, análisis forense informático, aspectos jurídicos del derecho probatorio, evidencia y prueba digital, que tributan sus teorías a la auditoria forense.

Ahora bien, los hallazgos se compararon con las distintas posiciones planteadas en el Fundamento Teórico, que expone de manera integral como la ciencias forenses se articulan con el derecho; del mismo modo, como el estudio sistemático de datos digitales se convierte en una disciplina forense cuando se relaciona con la investigación y el enjuiciamiento de un delito; se parte de esta mirada para caracterizar los aportes que se derivan del ejercicio de la auditoria forense y el análisis informático forense que le asiste, como metodología en la detección de fraudes informáticos.

Análisis de la información

El proceso de selección y análisis de la información documental incorpora un proceso de discriminación, que involucra separar material mediante elección o descarte. Para ello se empleó la dinámica que brinda el índice bibliográfico, pues esta permite vincular la fuente con la investigación de manera objetiva, valorarla, segregarla y relacionarla con los objetivos de investigación y descartar aquella que no cumple con los criterios ya definidos. Esta metodología permitió analizar las diferencias y semejanzas de los postulados planteados, así como una visión clara sobre la naturaleza del problema, en cuanto a sus orígenes, sus implicaciones, su funcionamiento y el consecuente efecto.

Resultados y discusión

Los factores de riesgo asociados al fraude deben evaluarse considerando siempre el ambiente y operatividad de la organización; debe tenerse igualmente una comprensión del negocio, así como su entorno económico y del mercado general en el que opera; ello permitirá determinar la presencia de otros factores de riesgo de fraude, si los hubiera; y la existencia y efectividad de controles mitigantes. Los hechos o circunstancias que pueden constituirse como factores de riesgo de fraude, pueden tener más o menos importancia, dependiendo de su contexto, por tanto, es probable que una pequeña organización manejada por sus propietarios cuente con estructuras de gobierno corporativo y sistemas de control interno menos sofisticados que una gran organización.

Volumen 06 - N° 02, Julio - Diciembre 2021
Depósito Legal N° DC2017000305/ISSN: 2542-3142

En concordancia con lo planteado, elementos básicos como la supervisión independiente de la administración, como el que aplica un comité de auditoría eficaz, y la segregación de funciones entre las funciones operativas, contables e informáticas claves, no están suficientemente desarrolladas, y es probable que no sean prácticas comunes en pequeñas organizaciones. Ahora bien, en una organización de gran tamaño, tales asuntos pueden ser motivo de preocupación, pero en una más pequeña, su impacto potencial en el riesgo de fraude, puede ser equilibrado, al menos parcialmente por la participación más cercana del propietario, así como la influencia que marca su propia cultura organizacional.

En este contexto, el entorno del fraude informático y la aplicación de las ciencias forenses en entornos electrónicos y digitales, está cambiando y desarrollándose significativamente; para hacer frente a la gestión del delito cibernético, en cuanto a: identificar, recopilar, recuperar, analizar y documentar, es necesario considerar procesos y procedimientos más eficaces y eficientes en las investigaciones digitales.

El desarrollo de nuevas tecnologías y entornos para posibles fraudes, como los avances en la informática de alto rendimiento, la bigdata, la nube y la prevalencia de las redes sociales, así como el uso ubicuo de las tecnologías móviles, significan que es necesario, considerar las herramientas y técnicas disponibles para un auditor forense que desarrolle actividades en el área digital; es necesario entonces, mejorar el uso de los recursos disponibles y superar las capacidades y limitaciones de las herramientas forenses que se utilizan actualmente, y seguir desarrollando el esquema metodológico y de investigación científica que la auditoria coloca a disposición de las ciencias forenses.

En consecuencia, el alcance de la auditoria y la evidencia recopilada y documentada deben ser capaces de soportar los desafíos que puedan presentar las partes afectadas; estos aspectos en conjunto, cumplen con el desarrollo del primer objetivo de la investigación al configurar a la auditoria forense como herramienta en la detección en los casos de fraude informático; ahora bien, la auditoría forense como fundamento preventivo y detectivo, no es la única metodología para acometer y mitigar el fraude, pero se constituye, con toda seguridad, en una metodología que extiende un aporte muy valioso para la lucha efectiva contra ese tipo de actividad delictiva.

En este sentido, los administradores de sistemas y el personal de seguridad también deben tener un conocimiento básico de cómo las tareas administrativas rutinarias del sistema y la red pueden afectar tanto el proceso forense, como la capacidad posterior de recuperar datos, que pueden ser críticos para la identificación y el análisis de un incidente de seguridad, aspectos como la frecuencia de los respaldos, así como su adecuado resguardo y ubicación, son esenciales.

Ahora bien, refiriéndonos a la relación intrínseca entre el derecho y los aspectos de carácter tecnológico e informático, esta impone retos importantes que deben ser atendidos desde la legislación local e internacional, haciendo uso entre otras, de las mejores prácticas existentes para el sector, así como la aplicación de normas de aceptación general, que permitan dar un tratamiento uniforme a los eventos de fraude informático que afectan a la sociedad en general.

Es así, como el desarrollo tecnológico ha obligado a los legisladores en términos globales, a replantear algunas figuras tradicionales de delitos, e incluso a crear nuevos tipo delictivos que permita proteger los derechos y libertades ciudadanas. En este orden, se habla ahora de delitos informáticos, en su mayoría como delitos de alto riesgo e impacto, los cuales se facilitan por el uso del internet y difieren de los tradicionales por utilizar medios informáticos para su consumación, o por atacar dichosa sus sistemas o sus soportes.

Por su parte, el proceso penal venezolano, según lo expuesto por Palao (2013), incorpora una fase investigativa en la cual el Ministerio Público asegura los elementos materiales y realiza de manera objetiva los análisis y pruebas que las instancias jurisdiccionales exijan, acción esta, que en conjunto conlleva a la formación de la prueba, ejercicio al que la doctrina jurídica denomina como prueba de cargo. El proceso de recabar y asegurar materiales y fuentes de prueba, es lo que se conoce como cadena de custodia.

Para recabar estas pruebas el Ministerio Público venezolano (2017), afirma que es necesaria la inspección y la actividad de investigación que conduce a la confirmación del estado de las cosas ubicados en los espacios donde se cometió un hecho punible o donde se presume pudo haberse materializado, planificado, guardado o encubierto y, en los cuales se

Volumen 06 - N° 02, Julio - Diciembre 2021
Depósito Legal N° DC2017000305/ISSN: 2542-3142

puedan hallar evidencias materiales e incluso puedan identificar a sus autores; en este orden, los materiales recogidos deben someterse con rigurosidad a la cadena de custodia, previo el cumplimiento de los extremos de ley para salvaguardar las garantías constitucionales.

Por consiguiente, toda información con valor probatorio que es almacenada y transmitida de forma digital o binaria, reúne las características de una prueba digital; en este contexto y atendiendo uno de los objetivos de la presente investigación relativo a describir los principios generales del derecho probatorio y su relación con la auditoria forense para los casos de fraude informático, pasa por considerar como lo refiere Ronderos (2015), los principios probatorios de carácter esencial, que detallan elementos básicos e imprescindibles al momento del análisis particular de cada evidencia y prueba:

- Necesidad de la prueba.
- Eficacia jurídica y legal de la prueba
- Unidad de la prueba
- Comunidad de la prueba
- Interés público de la función de la prueba
- Lealtad y probidad o veracidad de la prueba
- Contradicción de la prueba
- Igualdad de oportunidades para la prueba
- Publicidad de la prueba
- Formalidad y legitimidad de la prueba
- Preclusión de la prueba
- Inmediación de la prueba.

La valoración y apreciación de la prueba, se constituye en un proceso que debe ser suficientemente razonado y motivado; al ejercer esta acción, en apego irrestricto a la ética y a la realidad de los hechos, se marca distancia desde lo subjetivo y discrecional, por tanto, la decisión del Juez se encontrara apegada a pleno derecho; estas pruebas por lo general aportan información y/o hechos de manera directa o indirecta al problema procesal, por esta razón los autores y responsables del hecho delictivo hacen su mejor esfuerzo para ocultar o alterar las evidencias de fraude, siendo necesario de la administración de justicia obtengan suficientes garantías, tanto en la colección de evidencia, en la cadena de custodia y en el análisis forense para impedir que la evidencia se corrompa una vez identificada.

De esta manera, el cumplimiento de los principios probatorios en el tratamiento de los hallazgos de auditoría y su consecuente evidencia, es decisivo antes de colocar las pruebas a disposición del administrador de justicia, por esta razón, la investigación y sus resultados deben ser objetivos y detallados, lo cual permitirá demostrar los ilícitos en los cuales incurrieron la, o las personas investigadas, así como las relacionadas con la ocurrencia del fraude.

Ahora bien, al referirse a las oportunidades de mejora en los procedimientos de auditoria forense en ambiente TI, incluidas como parte de los objetivos de esta investigación, revisten gran transcendencia toda vez que permitirá desarrollar investigaciones con altos niveles de efectividad, al tiempo que proporcionan y aseguran el valor legal de las evidencias obtenidas y, que finalmente puedan ser presentadas ante responsables de seguridad integral de las organizaciones, autoridades investigativas y policiales, así como en los tribunales de justicia.

La auditoría forense aplicada a la informática, respalda las acciones de resolución de problemas, monitoreo, recuperación y protección de datos; además, ante la ocurrencia de un delito, el análisis informático forense, se conforma como el método para recopilar, analizar y archivar datos como prueba ante la instancia judicial competente. Aunque es escalable a muchos dominios de las tecnologías de la información, especialmente arquitecturas corporativas modernas, el análisis forense informático puede ser un desafío cuando se aplica a entornos no tradicionales, que no se encuentran conformados por tecnologías actualizadas o están diseñados bajo esquemas o modelos (de hardware y software) que no brindan capacidades adecuadas

Volumen 06 - N° 02, Julio - Diciembre 2021
Depósito Legal N° DC2017000305/ISSN: 2542-3142

de almacenamiento o auditoría de datos; asimismo, se introduce una mayor complejidad si los entornos se diseñan utilizando soluciones y protocolos privativos, lo que limita la dinámica con la que se pueden utilizar los métodos forenses modernos.

En este contexto, el análisis forense informático que actúa en apoyo a la auditoría, recopila dos tipos básicos de datos; uno de ellos, los datos persistentes, que son aquellos que se almacenan en un disco duro local (u otro medio) y se conservan cuando se apaga la computadora; los otros, los datos volátiles, que son cualquier dato que se almacena en la memoria, o que existe en tránsito, que se perderá cuando el equipo informático se apague. Los datos volátiles residen en registros, caché y memoria de acceso aleatorio; dado que los datos volátiles son efímeros, es fundamental que un investigador conozca formas fiables de capturarlos.

Bajo estas premisas, las redes de tecnología de la información, que operan a través de los mecanismos de intercambio de datos, los dispositivos de almacenamiento de datos y los componentes informáticos en general, proporcionan una buena base para crear el panorama utilizado para respaldar una auditoria forense en un entorno informático de manera eficaz. Sin embargo, los entornos de los sistemas de información modernos, no se pueden configurar fácilmente para adaptarse a los programas forenses. Los protocolos no estandarizados, las arquitecturas heredadas que pueden tener varias décadas de antigüedad y las tecnologías licenciadas no actualizadas o extintas, pueden combinarse para hacer que la creación y operación de un análisis informático forense incluido en un programa de auditoria, sea cualquier cosa menos un proceso sencillo y fluido.

En este orden, las mejores prácticas que se describen, no intentan reemplazar un enfoque específico del sector para la creación de un programa auditoría forense y un análisis informático forense, sino proporcionar orientación en lo que se refiere a cuestiones específicas de los sistemas de información. El alcance del detalle que exponen estas mejores prácticas, no es técnicamente exigente y puede ayudar a proporcionar una base para crear o aumentar las iniciativas de protección y recuperación de recursos de información existentes, y mejorar los resultados de las auditorias forenses que se desarrollen en un ambiente informático.

El objetivo de agrupar las mejores prácticas, es establecer un punto de referencia de calidad, principios y enfoques para la detección, preservación, recuperación, análisis, examen y uso de los resultados de la auditoria y de la evidencia digital con fines forenses.

Las mejores prácticas también sirven para alentar a los profesionales a adoptar una metodología coherente para promover y facilitar el intercambio de datos. Esto es particularmente importante dada la creciente necesidad de que los investigadores locales coordinen esfuerzos con sus contrapartes en el extranjero.

Los resultados del examen forense informático y la aplicación efectiva de herramientas y prácticas analíticas como lo señala Nigrini (2020), depende de manera crítica tanto de la integridad de los procedimientos seguidos como de la calidad del trabajo realizado; en consecuencia debe haber un Programa de Auditoría Forense y Análisis Informático Forense debidamente documentado que cubra todos los sistemas, procesos y métodos utilizados en el examen y presentación de informes de evidencia digital forense, y otros que se encuentre relacionados.

Al proporcionar los pasos y procedimientos detallados que se deben seguir durante un examen informático forense, dicho programa de auditoría no solo ayudaría a garantizar la coherencia del proceso, sino que además podría servir como un recurso de referencia importante para el personal que puede encontrarse en una situación de asistencia.

Una vez desarrollado el programa de auditoria, definidas sus fases, alcance, ambiente de control, análisis de riesgo, talento humano, pruebas e insumos, reportes y presentación, cronograma de ejecución; es preciso, expone Nigrini (2020), se apliquen en su desarrollo las prácticas que a continuación se describen:

- Planificación, análisis de riesgo y ambiente de control.
- Selección de equipo y asignación de actividades.
- Principios y responsabilidades.

Volumen 06 - N° 02, Julio - Diciembre 2021
Depósito Legal N° DC2017000305/ISSN: 2542-3142

- Integridad y autenticidad de datos.
- Insumos, equipos, aplicaciones y procesos.
- Modelos de buenas prácticas y/o estándares de procesos.
- Evaluación, revisión y ajustes del plan de trabajo.
- Análisis documental.
- Análisis y evaluación de evidencias.
- Desarrollo, evaluación, discusión y consideración de hallazgos.
- Informe preliminar.
- Informe de resultados.
- Plan de acciones correctivas.
- Compromisos y cierre.

Estas acciones, como se citó previamente no sustituyen práctica alguna, complementaran otras que reforzaran las actividades que enmarcan una auditoria forense en un ambiente informático, en procura de obtener la veracidad de los hechos; para ello debe considerarse el siguiente detalle:

- Tareas y análisis de campo
- Al realizar esta actividad, el auditor forense debe:
- Aplicar los principios y procedimientos forenses generales, necesarios para el tratamiento de pruebas digitales.
- No realizar ninguna acción que cambie la evidencia que se tiene, incluidos los datos en los medios de respaldo o en las computadoras.

- Asegurarse que solo personas calificadas tengan acceso a la evidencia digital.

En circunstancias excepcionales, se pudiese permitir que otros interesados accedan a los datos originales acopiados en una computadora de destino u otros medios, para ello es necesario documentar la identificación de los analistas e investigadores, legalidad y autorización del proceso, tiempo de contacto e interacción con la evidencia, cumplimiento de protocolos y pruebas realizadas, equipos empleados, entre otros. En tales casos, es vital que todas y cada una de las personas que accedan a los datos sean competentes para hacerlo y competentes en enterar pruebas que expliquen la relevancia y las implicaciones de sus acciones.

Documentar todas las actividades relacionadas con la incautación, acceso, almacenamiento y transferencia de evidencia digital y preservar un registro. Un tercer experto independiente debería poder examinar esos procedimientos documentados de manera que si este tercero repitiera el proceso, debería llegar al mismo resultado.

Es importante tener en cuenta, que como investigador en posesión de evidencia digital, un auditor es responsable de todas las acciones tomadas con respecto a esta evidencia digital. Como parte responsable, debe asegurarse que se cumplan estos principios inmersos en las mejores prácticas de auditoria e informática forense.

- Principios y responsabilidades
- Mantenimiento, integridad y autenticidad de datos.
- Protocolos de prevención que eviten la contaminación y pérdida de datos.
- Documentación adecuada y completa, e
- Implementación de una metodología científica sistemática
- En relación a la responsabilidad ética y profesional que le asiste, su enfoque debe dirigirse a:
- Mantener su objetividad.

Volumen 06 - N° 02, Julio - Diciembre 2021
Depósito Legal N° DC2017000305/ISSN: 2542-3142

- Presentar hechos con precisión.
- No ocultar ningún hallazgo ya que tales acciones pueden distorsionar los hechos.
- Emitir opiniones solo por lo que pueda demostrarse razonablemente.

Interidad de los datos

Análisis de archivos: borrado y recuperación de datos, firmas, documentos ofimáticos, archivos gráficos, archivos de medios (audio y video), códigos ejecutables.

Análisis forense de sistemas: versiones del sistema operativo, información volátil, orden y tipos de información volátil presente en el incidente, análisis forense de la memoria RAM, análisis de particiones NTFS y FAT, papelera de reciclaje, cookies, historial de navegación de internet, metadatos, cadenas de caracteres, registro del sistema operativo, servidores, datacenter, baterías de respaldo, temperatura.

Análisis forense en redes e internet: características de la red, protocolos, examen y comprobación de direcciones IP, herramientas de trazas de red, análisis de trafico de red, correo electrónico, clúster, computación en la nube, internet de las cosas, redes sociales, blockchain, bigdata, respaldos, redundancia.

- Autenticidad de datos
- Validez
- Conformidad
- Veracidad de la información
- Libres de contaminación
- Documentación completa
- Metodología científica

Soporte de datos. Análisis por niveles: dispositivos físicos, volúmenes y particiones, sistema de archivos, bloque de datos, metadatos y nombres de los archivos.

- Manejo de incidentes
- Acciones permitidas y acciones no consentidas.
- Contactos
- Accesos lógicos y físicos
- Políticas de seguridad de datos: password, respaldos, ambientes compartidos, VPN, bloqueos de puertos y navegación, acceso remoto, intranet.
- Procedimientos para trabajar con investigadores.
- Grabación de eventos.
- Política y/o procedimientos de acción correctiva.
- Amenazas digitales: evaluación de riesgos, posibles motivaciones del delincuente, amenazas internas y externas, estrategias del atacante.

Equipos y procedimientos

- Todo el equipo utilizado durante el trabajo de análisis forense debe ser apropiado para el propósito y recibir un mantenimiento adecuado dadas las consideraciones de carácter operativo.
- Solo se deben utilizar herramientas, técnicas y procedimientos evaluados adecuadamente para un examen forense de tecnología digital.
- Todos los medios utilizados para hacer análisis y copias deben ser equipos forenses certificados.
-

Volumen 06 - N° 02, Julio - Diciembre 2021
Depósito Legal N° DC2017000305/ISSN: 2542-3142

- Revisión del programa
- Todo el trabajo realizado debe estar sujeto tanto a una revisión técnica, así como a una revisión de carácter administrativo.
- La revisión técnica debe considerar:
- La validez de todos los hallazgos críticos del examen y todos los datos brutos utilizados en la preparación de la declaración / informe
- Si las conclusiones extraídas están justificadas por el trabajo realizado y la información disponible o,
- Si las circunstancias justifican pruebas independientes adicionales
- Se debe realizar un registro escrito de la revisión técnica y conservarlo con los registros del caso.

La revisión administrativa debe realizarse para garantizar que las necesidades de los solicitantes se aborden adecuadamente, que las políticas se cumplan sin limitaciones y que el documento de informe cumpla con los estándares apropiados.

Informe final

El informe final debe proporcionar al lector toda la información relevante de manera clara, concisa, estructurada e inequívoca. Las descripciones deben hacerse en un lenguaje sencillo evitando la expresiones de carácter técnico siempre que sea posible, asimismo el informe debe contener hallazgos fácticos.

También se debe incluir interpretación y opinión de expertos, claramente identificadas en el informe. Si el informe se utilizará en un litigio, el estilo y el contenido de los informes escritos deben cumplir con los requisitos del sistema de justicia penal que aplique según las circunstancias.

Los cambios en las plataformas de tecnología de la información (TI), así como los presentes en los distintos medios de almacenamiento, en las aplicaciones de software, y en la legislación en general, de las que se vale la auditoria forense, impulsa el empleo de metodologías, procesos y estándares, que procuren la recuperación de la información sin la presencia de elementos que la distorsionen, y sobre todo, acciones que en conjunto aseguren que las tareas incorporadas en la metodología aplicada se realizaron sin ningún tipo de restricciones, y que tributen sin más limitaciones que las que impone la ley, a la conformación de pruebas que coadyuven no solo a la detección de ilícitos asociados al entorno informático y su consecuente mitigación, sino que contribuya a su penalización a través de tribunales de justicia; en términos generales la auditoria forense en su perfil preventivo y detectivo, se configura como fundamento metodológico en la detección de casos de fraude informático.

Conclusiones

Los procedimientos de auditoría forense aplicados para la detección de fraudes informáticos deben contar con una metodología adaptable y comprensible, que aseguren la confiabilidad de los resultados obtenidos, dicha confiabilidad incluye la trazabilidad, la confidencialidad, la autenticidad, la integridad y el no repudio de los datos o de la información resultante de la auditoría practicada.

El fundamento metodológico en el que se apoya la auditoría forense para la detección de casos de fraude informático, involucra componentes de seguridad y resguardo, garantía que los elementos probatorios ofrecidos como prueba son confiables, es decir, no han sido expuestos a modificación, sustracción o eliminación de datos en ninguna de sus partes, a objeto que no reflejan inexactitud en cualquiera de las fases de la investigación.

Es importante que en las organizaciones, se implementen prácticas que permitan la detección oportuna del fraude, en cuya gestión se encuentren presentes actividades de planificación y estrategia, que incorporé a su vez, la medición y evaluación de riesgos como elemento intrínseco de gestión, sumado a controles internos adecuados, que en conjunto limiten la presencia de cualquier tipo de fraude.

Volumen 06 - N° 02, Julio - Diciembre 2021
Depósito Legal N° DC2017000305/ISSN: 2542-3142

La auditoría forense, como disciplina auxiliar de la criminalística, no determina responsabilidades no aplica sanciones, ni hace referencia a ningún tipo de castigo, este tipo de auditoría, efectúa análisis e investigaciones que conlleven a develar la realidad de los hechos relacionados al fraude informático, y conformar pruebas relativas a su ejecución, desarrollo y materialización. Es importante se consideré, que las técnicas forenses no reemplazarán a las normas, reglas o procedimientos relacionados a cada especialización, por lo tanto nunca se debe dejar de aplicar los conocimientos relacionados a la especialidad que le asiste, tales como contabilidad, finanzas, informática, sistemas, aseguramiento y control, así como el apoyo decisivo de la legislación pertinente.

En otro contexto y desde la perspectiva la administración de justicia, la prueba digital debe considerar los principios rectores jurídicamente hablando que blindan su prestación, pero también ha de reconocer las diversas formas en que se manifiesta esta prueba digital; de igual manera, legisladores y jueces deben comprender los protocolos que permiten asegurar que los datos colectados y presentes en las evidencias digitales no hayan sido modificadas y/o alteradas de forma indebida por alguna de las partes. Las TI nos facilita herramientas y aplicativos tecnológicos e informáticos, que permite garantizar el origen e integridad de los datos incorporados en un documento digital, conformándose en la prueba digital por excelencia.

El avance en la conexión necesaria que se da entre lo jurídico y lo informático, viene generando material e insumos importantes que fortalecerán la doctrina que sobre el particular se desarrolle; ahora bien, esta información producto de decisiones judiciales, resoluciones y normativas gubernamentales, casos de estudio e incluso estándares y/o buenas prácticas en el ejercicio del derecho informático a nivel local y mundial, proveerá de herramientas necesarias para la adecuación de la legislación en este ámbito, la cual debe ir a la par del avance que marque las tecnologías de la información.

En otro orden de ideas, la ejecución de un plan congruente de auditoria, cuyo enfoque dirija su atención hacia el análisis forense digital, demanda herramientas tecnológicas especializadas y de un equipo auditor multidisciplinario, pero igualmente requiere de una metodología particular que incorpore buenas prácticas y tendencias que marca la investigación forense a nivel mundial,

muy particularmente la enfocada a la informática; estos aspectos implican gran relevancia, por cuanto ello garantizaría el cumplimiento de los requerimientos legales y técnicos que exigen los procesos de auditoria forense; asimismo, en la tarea de detección del fraude informático, es imprescindible seguir una metodología segura y eficiente, que coadyuve a la obtención de resultados tangibles y objetivos, elementos que permitirá a la administración de justicia su valoración sin objeción ni salvedades.

La auditoría forense, proporciona los principios y técnicas que coadyuvan al proceso investigativo de hechos delictivos, incluidos los de carácter tecnológico; en este orden, se recomienda, considerar en su planificación y ejecución, prácticas y/o rutinas que permitan identificar, recuperar, reconstruir o analizar la evidencia sujeta a examen.

Referencias bibliográficas

Acosta, M.; Benavides, M. y García, N. (2020). Delitos informáticos: Impunidad organizacional y su complejidad en el mundo de los negocios. Revista Venezolana de Gerencia, vol. 25, núm. 89, 2020. Universidad del Zulia, Venezuela.

Acurio, S. (2016). Evidencia Digital en el Proceso Judicial. Publicación en línea.

Disponible en: https://www.sites.oas.org/cyber/Documents/2016%20-20Digital%

20%el%Proceso%20Judicial-Santiago%20Acurio.pdf [Consulta: 2019, diciembre 13]

Aguilar, S. (2019). La prueba digital en el proceso judicial. Ámbito civil y penal. Bosch Editor. Octubre 2019. Barcelona. España.

Casey, E. (2011). Digital Evidence and Computer Crime, Third Edition. 2011 Eoghan Casey. Published by Elsevier Inc. Baltimore, Maryland, USA

Casey, E. (2019). The chequered past and risky future of digital forensics, Australian Journal of Forensic Sciences, Vol. 51:6, pp. 649-664. Australian Academy of Forensic Sciences. Sidney, Australia.

Chisum, J. & Turvey, B. (2017). Crime Scene Processing. Forensic Investigations (pp.125-156).

Cressey, D. (1961). The prison; studies in institutional organization and change. Holt, Rinehart and Winston; Edición: First Edition (1961). New York. U.S.A.

Devia, E. (2017). Delito informático. Tesis Doctoral presentada para la obtención del Grado de Doctor en Derecho por la Universidad de Sevilla. España

Márquez, R. (2018). Auditoria Forense. Instituto Mexicano de Contadores Públicos. IMPC. México. D.F.

Martínez, J. (2020). Métodos de Investigación Financiera. Guía N.° 1 Conceptos y Generalidades. Auditoría Forense. OEA-CICAD.

Mayer, L. y Oliver G. (2020). El delito de fraude informático: Concepto y delimitación. Revista Chilena de Derecho y Tecnología. Vol. 9 N° 1 (2020). pp. 151-184. Santiago. Chile

Ministerio Público. (2017). Manual Único de Procedimientos en Materia de Cadena de Custodia y Evidencias Físicas. Fiscalía General de la República Bolivariana de Venezuela y Ministerio del P.P para el Interior, Justicia y Paz. Caracas. Venezuela.

Nelson, B.; Phillips, A. & Steuart, Ch. (2019).Guide to Computer Forensics and Investigations, 6th Edition. Cengage Learnig. Boston. Mas. 02210. USA.

Nigrini, M. (2020). Forensic Analytics: Methods and Techniques for Forensic Accounting Investigations (Wiley Corporate F&A). 2nd Edición (may-2020). Edit. Wiley. US.

Palao, J. (2013). Los medios informáticos como medios de prueba libre en el procedimiento civil ordinario en Venezuela. Trabajo Especial de Grado en la Especialización de Derecho Procesal. Universidad Católica Andrés Bello UCAB. Caracas. Venezuela.

Posada, R. (2017). El cibercrimen y sus efectos en la teoría de la tipicidad: de una realidad física a una realidad virtual. Revista Nuevo Foro Penal Vol. 13, No. 88, enero-junio 2017, pp. 72-112. Universidad EAFIT, Medellín. Colombia.

Ronderos, J. (2015). La prueba digital en el contexto jurídico actual. BID, Documento en línea. Disponible en: https://www.deceval.com.co/portal/page/portal/Home/Marco_Legal/Eventos/Presentacion_Deceval_JGRFINAL.pdf [Consulta: 2020, marzo 16]

Volumen 06 - N° 02, Julio - Diciembre 2021
Depósito Legal N° DC2017000305/ISSN: 2542-3142