AUDITORÍA FORENSE APLICADA LA TECNOLOGÍA

Álvaro Fonseca Vivas PhD

RESUMEN

La auditoría forense aplicada a la tecnología en especial a la informática que según con los avances de los medios electrónicos de datos en forma virtual y de la globalización de la información, donde juega un papel muy importante y fundamental en la detección, investigación y resolución de crímenes económicos y financieros que involucran incidentes, fraudes y delitos informáticos de seguridad, proporcionando evidencias físicas o elementos materiales probatorios – EMP o pruebas judiciales técnicamente solidas para el apoyo de la administración de justicia en casos judiciales, legales y administrativos determinando los victimarios y el impacto que este ocasiona.

Palabras claves: Tecnología, técnico, ingeniería, informática, fraudes informáticos, hacker, cracker, auditoría, forense, crímenes.

ABSTRACT

The forensic audit applied to technology, especially computer technology, which according to the advances of electronic data media in virtual form and the globalization of information, plays a very important and fundamental role in the detection, investigation and resolution of economic and financial crimes involving incidents, fraud and computer security crimes, providing physical evidence or evidentiary material elements - EMP or technically solid judicial evidence to support the administration of justice in judicial, legal and administrative cases, determining the perpetrators and the impact that this causes.

Keywords: Technology, technical, engineering, computer science, computer fraud, hacker, cracker, audit, forensics, crime.

CONCEPTOS DE TECNOLOGÍA

La Tecnología y en este caso la Informática se refiere a un conjunto de conocimientos, herramientas, procesos y sistemas relacionados con el manejo y procesamiento de la información mediante el uso de las computadoras o Personal Computer - PC y otros dispositivos electrónicos. También se le conoce como Tecnología de la Información (TI).

Si bien la Tecnología Informática abarca diversos aspectos, como el hardware (componentes físicos de los equipos informáticos), el software (programas y aplicaciones), las redes y los sistemas de comunicación, la seguridad informática, la gestión de datos y a la infraestructura tecnológica en general.

Por ello podríamos mostrar algunos ejemplos de áreas dentro de la Tecnología Informática que incluyen entre otros lo siguiente:

1.- Desarrollo de software: Que comprende la creación, diseño, programación y mantenimiento de programas y aplicaciones informáticas, tanto para uso general como para un uso específico de una organización.

2.- La administración de redes: La cual se encarga de establecer y de gestionar las conexiones de la red entre dispositivos informáticos, asegurando la comunicación eficiente y segura entre ellos.

3.- La seguridad informática: Esta se enfoca en proteger los sistemas informáticos y la información contra las amenazas y de los ataques cibernéticos, implementando medidas de seguridad como firewalls, cifrado, autenticación y políticas de acceso.

4.- Las Bases de datos: Que implica el diseño, la implementación y la gestión de los sistemas de almacenamiento y organización de datos, permitiendo su recuperación eficiente y segura.

5.- La administración de sistemas: Este incluye el monitoreo, mantenimiento y optimización de los recursos informáticos, como son los servidores, los sistemas operativos y los servicios de mantenimiento de estos, para garantizar su correcto funcionamiento y la disponibilidad de dichos servicios.

Por lo tanto, la Tecnología Informática tiene un papel fundamental en la sociedad actual, debido a que, esta se utiliza en casi todos los aspectos de nuestra vida diaria, tanto en el ámbito personal como en el empresarial. Facilita la comunicación, el acceso a la información, la automatización de tareas, el procesamiento de datos y muchas otras actividades que nos permiten ser más eficientes y productivos en las actividades rutinarias.

Algunos de los diferentes autores lo definen así: Methere: Conocimiento aplicado a propósitos prácticos.

Dupree: Define que la tecnología es como un sistema de información que conecta al homo sapiens con su ambiente. Donde la finalidad de la tecnología seria la búsqueda de una verdad útil. Mientras que Falcott. (Desde la sociología): Señala que la tecnología es la capacidad socialmente organizada para controlar y alterar activamente objetos del ambiente físico en interés de algún deseo o necesidad humana. Por otro lado, Sábato (desde la economía) ve como un conjunto ordenado de conocimientos necesarios para la producción y comercialización de bienes y servicios, como también entre otros se encuentra Galbraith (The new industrial state) quien menciona que la tecnología es la aplicación sistemática del conocimiento científico o de otro tipo de conocimiento organizado, a tareas practicas.

CONCEPTO DE TECNOLOGÍA

Resulta impresionante cómo la tecnología en especial la tecnológica evoluciona con cada día que pasa. Y debido a esta evolución, su conceptualización resulta cada vez más rica y variada. Muchos han sido los autores que se han decidido a sentar las bases del término. Amplias y variadas han sido estas definiciones. La gran mayoría la describen y la analizan como un fenómeno científico-social. Otras caen en la disyuntiva de considerarla como una ciencia aplicada o tomarla como un proceso autónomo, más no independiente, respecto a la ciencia. Por otro lado, hay quienes afirman que es necesario diferenciarla muy bien de la técnica. Ésta, posee una connotación más artesanal, común, sin una profunda interrelación con el hecho científico, y que busca solucionar las situaciones concretas e inmediatas a las cuales

se aplica. Mientras que la tecnología no puede obviar este aspecto intrínsecamente científico.

La tecnología en este caso la informática, no solamente invade toda la actividad industrial, sino que también participa profundamente en cualquier tipo de actividad humana, en todos los campos de actuación. El ser humano, moderno utiliza en su comportamiento cotidiano y casi sin percibirlo una inmensa avalancha de contribuciones de la tecnología: el automóvil, el reloj, el teléfono, las comunicaciones, entre otros. A pesar de que existe conocimiento que no puede ser considerado conocimiento tecnológico.

Por lo tanto, la auditoría forense aplicada a la tecnología informática es una disciplina especializada que tiene como objetivo el de recopilar, analizar y presentar evidencia digital en casos legales con las pruebas judiciales, elementos materiales probatorios – EMP o evidencias físicas o digitales. Donde se enfoca es en investigar y descubrir fraudes, delitos informáticos o incidentes de seguridad que hayan ocurrido en sistemas o redes informáticas de cualquier tipo de organización o de entidad, por lo tanto, nunca puede ser preventiva.

Donde la auditoría forense aplicada a la tecnología informática, esta utiliza técnicas y herramientas especializadas por expertos en este campo para examinar y recuperar datos de dispositivos electrónicos, como computadoras, servidores, dispositivos móviles, sistemas de almacenamiento, entre muchos otros, dependiendo el caso de posible fraude o delito y cullo resultado será entregado o presentado ante una corte o tribunales de justicia. También implica analizar registros y archivos de registro, identificar intrusiones, seguir el rastro digital de actividades sospechosas y el de verificar la integridad de la evidencia digital.

Es por ello por lo que se pueden identificar los objetivos principales de una auditoría forense aplicada a la tecnología informática y entre ellos tenemos:

1.- Conocer o indagar sobre la organización en la cual se investigará el fraude o delito con base a las presunciones e indicios de ellos.

2.- Identificar y recolectar la evidencia digital o los elementos materiales probatorios y pruebas judiciales de manera forensemente válida.

3.- Analizar y examinar la evidencia para comprender los hechos de lo ocurrido.

4.- Determinar la causa o la raíz del incidente o del delito informático.

5.- Presentar los hallazgos y las evidencias de manera clara y concisa en un informe o en un dictamen pericial forense.

A ello se observa, que la auditoría forense aplicada a la tecnología informática es una herramienta importante en el ámbito legal, debido a que, esta proporciona pruebas digitales que pueden ser utilizadas en investigaciones y litigios de crímenes económicos y financieros, determinando quienes son las víctimas y por lo tanto identificando a los victimarios incluyendo el impacto generado por ello. Además, también se utiliza en el ámbito de las organizaciones empresariales o entidades para evaluar la seguridad de los sistemas y con estos resultados encontrados y las lecciones aprendidas ayudar a prevenir en el futuro posibles incidentes.

Es importante destacar que la auditoría forense informática debe llevarse a cabo por profesionales capacitados y con experiencia en el campo, ya que requiere conocimientos técnicos especializados y el cumplimiento de procedimientos rigurosos para garantizar la validez y confiabilidad de la evidencia digital recopilada.

INTERRELACIÓN ENTRE CIENCIA Y TECNOLOGÍA

Es interesante ver cómo en tiempos actuales y a través del tiempo se ha hecho

difícil diferenciar la tecnología de la ciencia. Son dos actividades únicas, separadas, pero no divorciadas, con naturalezas muy específicas, pero con una profunda e íntima interrelación. De manera general, la ciencia sería el “por qué conocer,” el “por qué llegar más allá” y el “qué de las cosas y sus circunstancias”; una incansable búsqueda de la verdad. Mientras que la tecnología es el “cómo conocer”, el “cómo aplicar” los conocimientos adquiridos para resolver soluciones, crear cosas, con el fin de elevar cada día más la calidad de vida del hombre.

En los avances de la tecnología moderna es predominantemente científica, debido a que extrae sus fundamentos teóricos de la ciencia pura o básica. Los significados de los términos ciencia y tecnología han variado significativamente de una generación a otra. Sin embargo, se encuentran más similitudes que diferencias entre ambos términos. Donde si bien se han hecho diferenciar en el pasado hoy en día la ciencia y la tecnología son dos campos interrelacionados pero distintos que se enfocan en

diferentes aspectos del conocimiento y la aplicación práctica. Donde se presenta una forma de entender cada uno de estos campos:

1.- La Ciencia: La ciencia es un proceso sistemático de adquisición de conocimiento sobre el mundo biológico como natural y de cómo funciona. Esta se basa en la observación, experimentación, análisis y formulación de teorías y leyes que explican los fenómenos naturales. La ciencia busca comprender cómo y por qué ocurren las cosas en el universo, y se basa en siempre en evidencias y la aplicación del método científico para formular explicaciones verificables. Los científicos llevan a cabo por lo tanto sus investigaciones, realizan experimentos y recopilan datos para construir modelos y teorías que expliquen los fenómenos que han sido observados y de sus resultados.

2.- La Tecnología: por otro lado, la tecnología, se centra en la aplicación práctica del conocimiento científico para diseñar y crear herramientas, productos y sistemas que satisfacen las necesidades humanas y mejoran la calidad de vida. Donde la tecnología utiliza los principios y descubrimientos de la ciencia para desarrollar soluciones prácticas y aplicaciones concretas, que estas implican el uso de los conocimientos

técnicos y las habilidades para diseñar, fabricar y operar dispositivos, máquinas, software y sistemas que resuelven problemas y mejoran las actividades humanas en diversos campos.

Por lo que se puede decir que la ciencia busca comprender cómo funciona el mundo natural y se basa en el conocimiento científico adquirido a través de la investigación y el estudio. La tecnología, por su parte, aplica ese conocimiento científico para desarrollar soluciones prácticas y herramientas que ayudan a mejoran la sociedad y a satisfacer las necesidades humanas para un mejor vivir. La ciencia y la tecnología se influyen mutuamente, debido a que en los avances científicos a menudo estas impulsan el desarrollo tecnológico y en este caso el informático, y las aplicaciones tecnológicas pueden abrir nuevas áreas de investigación científica.

EL PAPEL SOCIAL DE LA TECNOLOGÍA

Algunos historiadores científicos argumentan que la tecnología no es sólo una condición esencial para la civilización avanzada y muchas veces industrial, sino que también la velocidad del cambio tecnológico en especial el informático ha desarrollado su propio ímpetu en los últimos siglos, que en tiempos modernos

hablamos de la robótica y de la Inteligencia Artificial - IA. Las innovaciones parecen surgir a un ritmo que se incrementa en progresión geométrica, sin tener en cuenta los límites geográficos ni los sistemas políticos.

Entre tanto, podemos aclarar un poco la diferencia entre la ciencia y la tecnología informática, en cuanto al medio social en el cual se desarrollan: En donde las comunidades que las sustentan tienden a valorar tanto el "conocer" como el "hacer". Es por ello por lo que el auditorio de la ciencia tiende a constituirse por científicos investigadores, mientras que el auditorio principal de la tecnología informática no está compuesto por investigadores netos sino por quienes buscan resultados de utilidad y que esta sea práctica.

Como es el caso de la robótica. La robótica es un campo interdisciplinario que utiliza distintas disciplinas para diseñar, construir y programar robots, y donde estos robots son máquinas programables que pueden realizar tareas de manera autónoma o semiautónoma, que tienen un impacto significativo en varios campos y sectores, incluyendo la industria, la medicina, la educación, la exploración espacial, la agricultura, la logística y el entretenimiento, entre muchas otras actividades rutinarias. Algunos beneficios y aspectos positivos de la robótica son:

1.- La Automatización y eficiencia: Los robots pueden realizar tareas de manera más rápida, precisa y eficiente que los seres humanos en muchas situaciones. La automatización robótica puede ayudar a optimizar procesos, aumentar la producción y reducir los errores.

2.- Las tareas peligrosas y entornos hostiles: Los robots pueden ser utilizados para realizar tareas peligrosas o en entornos hostiles, como la exploración espacial, la desactivación de explosivos, la limpieza de desechos tóxicos o el acceso a lugares inaccesibles para los humanos.

3.- La asistencia en la salud: Los robots pueden desempeñar un papel importante en la asistencia sanitaria, como la realización de cirugías precisas y menos invasivas, el apoyo a la rehabilitación física y el cuidado de pacientes en hospitales o residencias de ancianos.

4.- En la educación y el aprendizaje: Los robots educativos pueden ser utilizados como herramientas de enseñanza interactivas para fomentar el aprendizaje y el

desarrollo de habilidades en niños y adultos. También pueden ayudar en la investigación y experimentación científica.

Pero esto no es más que una manera figurada, porque también existen preocupaciones y desafíos asociados con la robótica, como es el impacto en el empleo, la ética de la inteligencia artificial, la privacidad y seguridad de los datos, y las implicaciones sociales, ambientales y económicas. Es importante abordar estos aspectos de una manera responsable y asegurar que la robótica y la inteligencia artificial se utilicen en un buen sentido para el beneficio de la sociedad en general.

Recordemos que la robótica es un campo emocionante y en constante evolución,

por lo que es necesario considerar tanto sus beneficios como sus implicaciones e impactos éticos y sociales a medida que avanza su desarrollo.

Desde este ángulo la Inteligencia Artificial – IA, es un campo de estudio que se enfoca en desarrollar sistemas y algoritmos capaces de simular y emular la inteligencia humana. Estos sistemas buscan aprender, razonar, percibir y tomar decisiones de manera similar a como lo hacen los seres humanos.

La IA ha experimentado un rápido avance en las últimas décadas y ha demostrado ser aplicable en una amplia gama de áreas, incluyendo la medicina, la industria, la conducción autónoma, la educación, la asistencia virtual, la traducción de idiomas, la detección de fraudes y muchos más aspectos en los cuales se está en desarrollo.

Hay como se ve, algunos beneficios y aspectos positivos de la Inteligencia Artificial – IA y estos son:

1.- La automatización y eficiencia: La Inteligencia Artificial – IA le permite la automatización de las tareas complejas y repetitivas o rutinarias, lo que conduce a una mayor eficiencia y productividad en diversos sectores.

2.- La toma de decisiones y análisis de datos: Los algoritmos de la Inteligencia Artificial – IA, pueden analizar grandes cantidades de datos para identificar patrones, tendencias y relaciones que podrían pasar desapercibidos para los sentidos de los humanos y esto permite tomar decisiones más informadas y basadas en datos.

3.- La mejora de la precisión: En los sistemas de la Inteligencia Artificial

– IA se pueden realizar tareas con una precisión y velocidad superiores a las capacidades humanas en muchas áreas, como el diagnóstico médico o la detección de fraudes o de delitos.

4.- La asistencia virtual y servicios personalizados: Los asistentes virtuales y los chatbots basados en la Inteligencia Artificial -IA le pueden brindar mejorar la experiencia del cliente y proporcionar servicios personalizados una vez este desarrollado este modelo.

Sin embargo, también existen preocupaciones y desafíos asociados con la Inteligencia Artificial - IA, como la privacidad de los datos, la falta de transparencia en los algoritmos, el impacto en el empleo y la ética en el uso de la Inteligencia Artificial - IA. Por lo tanto, es necesario abordar estos aspectos de una manera responsable y ética a medida que se avanza en el desarrollo de la IA.

Puede pensarse, que la Inteligencia Artificial – IA, es un campo con un gran potencial para transformar diversas áreas de la sociedad. Sin embargo, es importante considerar tanto sus beneficios como sus implicaciones en especial las éticas y sociales a medida que se continúa su desarrollo y aplicación.

Y es curioso que, paralelamente se viene trabajando por parte de los científicos para crear computadoras con células humanas, como es el caso de los Organides, que son estructuras tridimensionales de tejidos o células cultivadas en laboratorio que imitan características y funciones de órganos específicos en el cuerpo humano. Estos "miniórganos" artificiales se generan a partir de células madre o células especializadas que tienen la capacidad de autoorganizarse y formar estructuras similares a los órganos reales.

Los organoides representan una herramienta prometedora en la investigación biomédica, debido a que permiten estudiar los procesos biológicos y enfermedades de manera más precisa y controlada. Al replicar ciertos aspectos de los órganos humanos, los científicos pueden investigar cómo se desarrollan, funcionan y responden a diferentes tratamientos. Por lo que cada tipo de organoide está diseñado para imitar un órgano o tejido específico, como el cerebro, el hígado, el intestino, el riñón, los pulmones, entre muchos otros. Los organoides pueden utilizarse para estudiar la

formación de órganos durante el desarrollo embrionario, investigar enfermedades genéticas o estudiar respuestas a fármacos y terapias.

Queda definido que son una tecnología emergente y todavía hay desafíos técnicos y limitaciones en su desarrollo, pero ofrecen un gran potencial para la medicina regenerativa, el modelado de enfermedades y la personalización de tratamientos en el futuro. Este estudio de investigación nació con el doctor Thomas Hartung, de la Universidad Jhons Hopkins que menciona: "Me interesaba encontrar un modelo para entender el autismo y probar sustancias químicas relacionadas con esta condición. Por esos desarrollamos organoides cerebrales humanos, porque no queríamos hacer pruebas con ratas o ratones. Cuando vimos que los organoides cerebrales eran electrofisiológicamente activos, tuvimos la sensación de que estaban pensando. Y surgió la pregunta: ¿Qué pasa si les doy algo en qué pensar? Y así fue como empecé"[Thomas Hartung, MD, PhD, dirige la revolución en toxicología para alejarse de las pruebas en animales de más de 50 años a cultivos de organoides y el uso de inteligencia artificial. Recuperado de: https://www.eltiempo.com/vida/ciencia/entrevista-con-thomas-hartung-el-plan-para-crear-computadores-con-celulas- 767957]

HISTORIA DE LAS TELECOMUNICACIONES

Las telecomunicaciones se encargan del transporte de la información a grandes distancias a través de un medio o de un canal de comunicación por medio de señales. Por lo tanto, la misión de las telecomunicaciones es transportar la mayor cantidad de información en el menor tiempo de una manera segura. Eso se logra por medio de varias técnicas tales como la Modulación, codificación, Compresión, Formateo, Multicanalización, Esparciendo el espectro, entre otros.

VENTAJAS Y DESVENTAJAS DE LA TECNOLOGÍA

Para las décadas pertenecientes al siglo XX los logros tecnológicos fueron insuperables, con un ritmo de desarrollo mucho mayor que en periodos anteriores y en especial con la informática. La invención del automóvil, la radio, la televisión, el teléfono revolucionó el modo y calidad de vida y de trabajo de muchos millones de personas. Las dos áreas de mayor avance han sido la tecnología médica, que ha proporcionado los medios para diagnosticar y

vencer muchas enfermedades mortales, y la exploración del espacio, donde se ha producido el logro tecnológico más espectacular del siglo: por primera vez los hombres consiguieron abandonar y regresar a la biosfera terrestre.

Durante las últimas décadas y las transcurridas del siglo XXI, algunos observadores han comenzado a advertir sobre algunos resultados de la tecnología que también poseen aspectos destructivos y perjudiciales, sin contar que estos podrán reemplazar muchas labores que realizan los humanos.

CARACTERIZACIÓN DEL DELINCUENTE INFORMÁTICO

Cuando se habla de un delincuente informático, también conocido como ciberdelincuente o hacker malicioso, es una persona que utiliza habilidades y conocimientos técnicos en el campo de la informática o redes o utilizando la tecnología para cometer actividades delictivas en línea, donde esto puede incluir el acceso no autorizado a sistemas informáticos o en redes, el robo de información personal o financiera o confidencial la distribución de virus, gusanos o malware, el fraude y delitos cibernéticos, cometer fraudes y delitos económicos y financieros, espionaje, difundir malware, extorsionar a individuos o empresas, entre muchos otros actos ilegales, entre muchos otros. Pero también pueden ser grupos organizados con recursos significativos. La delincuencia informática es un problema cada vez más común en la sociedad actual, y las autoridades y empresas están trabajando para prevenir y combatir estos delitos, por ello la importancia de la Auditoria Forense aplicada a la tecnología.

Aunque en realidad los delincuentes informáticos pueden utilizar una variedad de técnicas y herramientas para llevar a cabo sus actividades delictivas. Esto incluye el uso de virus informáticos, ransomware, phishing, ingeniería social, ataques de fuerza bruta, exploits de seguridad y otros métodos para explotar vulnerabilidades en sistemas y redes. Se debe tener claro e importante, que no todos los expertos en seguridad informática o hackers son delincuentes informáticos. Existen hackers éticos, también conocidos como "sombreros blancos" o "hackers éticos", que utilizan sus habilidades para identificar y corregir vulnerabilidades en sistemas de forma legal y ética, con el objetivo de mejorar la seguridad en línea.

Para algunos autores, el sujeto activo de estos fraudes y delitos se encuentra conformado por un grupo de personas con una inteligencia y educación que superan el común con vastos conocimientos informáticos, sin embargo, que si se analizan los casos más celebres nos encontraremos con personas dotadas de altos conocimientos de informática y tecnología. Valga como ejemplo el caso de Kevin Mitnick, quien ha pasado más de la mitad de su vida defraudando mediante ordenadores. O el caso de Roberto Morris, estudiante de informática de la Universidad de Cornell cuyo Padre era un experto en seguridad del gobierno.

La extrañeza que causa es la de un mito, que el delincuente informático deba forzosamente poseer conocimientos profundos en la materia. Justo es decir que a juicio la computación se halla tan extendida hoy día que cualquier persona que posea conocimientos mínimos de informática y tenga acceso a un ordenador, incluso desde su casa. Puede realizar un fraude o un delito informático. Para el año de 1994, en su informe al Congreso de los Estados Unidos, la oficina de Asesoramiento Tecnológico del gobierno de ese país opinaba que las redes informáticas hacen de cada usuario básicamente un incidir con la potencia para asestar un golpe letal a lo sistemas de información. De allí las medidas de seguridad informática que se suelen tomar dentro de las entidades y en las organizaciones empresariales incluyendo a las personales, como ser la existencia de passwords, tarjetas magnéticas o con microchips de acceso al sistema e incluso reconocimiento de características biométricas y físicas de un individuo.

A partir de la experiencia comparada internacionalmente e incluso la nacional, los delitos informáticos y a los sujetos, pueden clasificarse en varias categorías según la naturaleza de la actividad delictiva, a continuación, se presentan algunas de las principales clases de delitos con tecnología informática:

Tabla 1.

Clases de delito y sujetos

Clase de delito	*Sujetos*
Delitos patrimoniales contra bancos y entidades financieras.	Empleados, en especial cajero o personal del área de sistema, exempleados.
Delitos de acceso ilegitimo o delitos de daños menores	Hackers, phreaks, usuarios descontentos
Daño o sabotaje informativo	Empleados de la empresa, o espías profesionales o industriales
Violaciones a la privacidad, tratamiento ilícito de datos personales.	Investigadores privados, Empresas de marketing, agencias de informes crediticios y de solvencia patrimonial
Violaciones a la propiedad intelectual del software y bancos de datos, con informes o compilaciones de datos.	Piratas informáticos o también usuarios (la copia amigable),empresas que realizan competencia parasitaria.
El acceso no autorizado, que involucra la obtención de acceso no autorizado a sistemas informáticos, redes o cuentas en línea.	Esto puede incluir el uso de contraseñas robadas, técnicas de hacking o vulnerabilidades de seguridad para ingresar a sistemas protegidos.
Robo de información, que implica la obtención y apropiación indebida de datos confidenciales, como información personal, datos financieros, secretos comerciales o propiedad intelectual.	Esto puede realizarse a través de ataques de phishing, programa maligno, ingeniería social u otras técnicas.
Fraude en línea, lo que comprende a una amplia gama de actividades fraudulentas, como estafas de phishing, estafas de compras en línea, fraude con tarjetas de crédito, fraude de identidad, fraudes de inversión, entre otros.	Estos delitos se llevan a cabo utilizando medios electrónicos y tecnológicos.

Clase de delito	*Sujetos*
Distribución de malware, queinvolucra la creación y distribución de software malicioso, como virus, gusanos, troyanos o ransomware.	Estos programas dañinos se utilizan para infectar sistemas, robar información, tomar el control de dispositivos o extorsionar a las víctimas exigiendo un rescate
Ciberacoso, que se refiere al uso de tecnología informática para acosar, intimidar o amenazar a individuos o grupos.	Esto puede realizar mediante la inclusión del acoso en redes sociales, el envío de mensajes ofensivos o difamatorios, la divulgación no autorizada de información personal sensible o la práctica de grooming (engaño a menores para obtener ventajas sexuales).
Sabotaje y vandalismo digital, esto implica la destrucción, alteración o interferencia malintencionada con sistemas informáticos, redes o datos.	Los delincuentes pueden eliminar o corromper información, interrumpir servicios en línea, atacar sitios web o realizar acciones que causen daños económicos o interrupciones operativas
Piratería informática, que se refiere a la violación de derechos de autor ypropiedad intelectual en el ámbito digital.	Esto incluye la distribución ilegal de software, música, películas, libros u otros contenidos protegidos por derechos de autor.
Espionaje informático, que se refiere a la recolección ilegal de información de sistemas informáticos o redes, con el fin de obtener información confidencial o secreta.	Individuos dentro de la organización que tienen acceso a información privilegiada y confidencial de las organizaciones empresariales o entidades que lo manejan incluyendo los sectores privados, públicos o sociales.

Estas son solo algunas de las clases de delitos informáticos más comunes, que en el panorama de los fraudes o delitos cibernéticos está en constante evolución, que pueden ser cometidos mediante el uso de la tecnología informática y las redes de comunicaciones, por lo tanto, los delincuentes utilizan nuevas técnicas y enfoques a medida que avanzan las tecnologías. En las diferentes jurisdicciones las leyes y regulaciones relacionadas con los delitos informáticos también varían según las mismas, aunque en la mayoría son muy laxas.

En definitiva, es preciso considerar que el delincuente informático no tiene necesariamente profundos conocimientos de computación, sino que es inducido a delinquir por la oportunidad o por la necesidad que se le presenta frente al uso diario del ordenador y la impunidad que éste le brinda, o por los conocimientos que éste tiene frente al resto del personal.

APLICACIÓN DE LA AUDITORIA FORENSE A LA TECNOLOGIA y CONCLUSIONES.

En fin, de cuentas, la auditoría forense aplicada a la tecnología informática realizada por personas especializadas como peritos o testigos expertos, y que se refiere a la aplicación de las técnicas y metodologías forenses en el ámbito de la tecnología de la información para investigar incidentes o crímenes económicos y financieros como los fraudes de seguridad, delitos informáticos o cualquier actividad sospechosa o de indicios relacionada con los sistemas y datos electrónicos.

Es importante entender que la auditoría forense su metodología está orientada hacia la transdisciplinariedad que es entendida desde dos sentidos uno es Multidisciplinariedad que es el dialogo de expertos y desde la interdisciplinariedad que es el dialogo de saberes, los cuales hace que se pueda trabajar con otras disciplinas porque los casos no solo los puede manejar un contador y en especial cuando se está ante investigaciones que en este caso son de tecnología informática, se debe apoyar de otras disciplinas para realizarlas. Así mismo esto está visto desde los aspectos del derecho y

una de sus ramas es el derecho penal y dentro de el la criminalística y la criminología que maneja las ciencias forenses, de otra parte dentro de la auditoria esta una rama que unida con las ciencias forenses nace la auditoria forense.

Cabe anticipar en términos generales, que la auditoría forense aplicada a la tecnología informática está en busca de recolectar, preservar y analizar evidencia digital con el fin de determinar qué ocurrió, quién estuvo involucrado o quiénes son los victimarios y victimas, cómo también de los hechos y las causas que se llevaron a cabo en un evento fraudulento o delito en particular, por lo que nunca es preventiva. El objetivo principal es obtener evidencias físicas, elementos materiales probatorios – EMP o de pruebas jurídicas técnicamente sólidas y confiables que puedan ser utilizadas en investigaciones legales o procesos judiciales, ante los jueces, jurados en la corte o en los tribunales.

Es por ello que la auditoría forense aplicada a la tecnología informática implica la aplicación de conocimientos técnicos en áreas como recuperación de datos, análisis de registros de actividad, análisis de malware o programa maligno, análisis de redes, análisis de sistemas operativos, manejo de los controles internos y análisis de bases de datos, entre muchos otros que sean requeridos en el caso investigado. Los auditores forenses expertos en informática utilizan herramientas especializadas y siguen procedimientos rigurosos para garantizar la integridad de la evidencia y cumplir con los requisitos legales, como también de las lecciones aprendidas, sin emitir juicios de valor y proporcionando el impacto que esto le genero a las víctimas como a la sociedad.

La utilización de un auditor forense que realice investigaciones criminales o financieras en el ámbito de la tecnología informática puede tener varias conclusiones y beneficios importantes, los cuales, se presentan como algunas conclusiones destacadas:

1.- En la identificación de evidencia: El auditor forense se debe encontrar capacitado para identificar, recopilar y preservar adecuadamente la evidencia física o los elementos materiales probatorios – EMP o las pruebas judiciales digitales relacionadas con un el caso o incidente o fraude o delito que se investiga. Esto incluye registros de actividad, archivos, correos electrónicos, registros de transacciones, metadatos y otros elementos que pueden ser relevantes para ser presentados ante la corte o en los tribunales y que estos sirvan a los jueces o al jurado para su veredicto de condena o de absolución de los victimarios.

2.- Un análisis técnico especializado: Los auditores forenses cuando se aplica a la tecnología de la informática, tienen conocimientos técnicos avanzados y herramientas especializadas para analizar y examinar la evidencia física o los elementos materiales probatorios – EMP o las pruebas judiciales digitales relacionadas de manera forense. Esto les permite descubrir patrones, reconstruir eventos o hechos, identificar vulnerabilidades de seguridad, rastrear actividades sospechosas y determinar la autoría de un fraude o un delito o incidente.

3.- La integridad y credibilidad de la evidencia: Un auditor forense sigue procedimientos rigurosos para garantizar la integridad y el buen manejo de la cadena de custodia de la evidencia física o los elementos materiales probatorios – EMP o las pruebas judiciales digitales relacionadas, que posteriormente serán presentados ante la corte o los tribunales judiciales. Esto asegura que los resultados de la investigación en crímenes económicos y financieros donde se utilizó la tecnología informática sean sólidos y confiables, lo que aumenta su credibilidad en un contexto legal o judicial.

4.- El apoyo a investigaciones y procesos legales: Los informes o los dictámenes periciales o forenses y los hallazgos generados por un auditor forense informático pueden utilizarse como evidencia en investigaciones criminales o procesos judiciales. Esto puede ayudar a fortalecer el caso legal, a disminuir la corrupción e impunidad, el respaldar las acusaciones o proporcionar una defensa sólida en los estados judiciales, dependiendo del contexto y el objetivo de la investigación.

5.- La mejora de la seguridad: A través de las experiencias aprendidas de cada caso investigado donde el auditor forense aplica la tecnología informática y con base a sus análisis y hallazgos, estos peritos o testigos expertos pueden identificar vulnerabilidades o debilidades en los sistemas y con base a sus informes y dictámenes periciales forenses sirven para implementar o realizar planes de mejoramiento en la seguridad para evitar futuros incidentes o fraudes o incidentes o delitos. Esto contribuye a fortalecer las defensas y en esta si el prevenir actividades maliciosas.

Por último, algunas de las tareas más comunes realizadas en una auditoría forense informática incluyen:

1.- La recopilación y preservación de evidencia digital de manera forense, asegurando su autenticidad y la debida cadena de custodia.

2.- El análisis y conclusiones de los registros y logs de sistemas para reconstruir los eventos o hechos y actividades relevantes que causaron el fraude o el delito.

3.- La recuperación de datos borrados o dañados para obtener información clave.

4.- El análisis del malware y/o programas maliciosos para identificar su funcionalidad como su procedencia y origen.

5.- El análisis de comunicaciones en redes para identificar patrones de tráfico o de actividades sospechosas.

6.- El examinar sistemas y aplicaciones en busca de vulnerabilidades o debilidades de seguridad que hayan ocasionado por la falta de controles y que hayan ocasionado el fraude o el delito informático.

7.- El manejo de sus papeles de trabajo y el documentar y presentar los hallazgos de una manera clara y concisa para su uso en investigaciones o procedimientos legales o la comparecencia en forma oral ante los tribunales o en la corte en caso de ser requerido.

Se debe tener en cuenta que la praxiología en la auditoría forense es una herramienta como se mencionaba transdisciplinar que es fundamental para el estudio y sistematización de los crímenes económicos, por lo tanto se vale de la praxiología, o ciencia de la decisión, para apoyar el dictamen pericial ante un juez o un jurado, si en su veredicto se absuelve o se condena a un victimario en la Corte, por ello la auditoría forense permite sistematizar las evidencias probatorias de forma más robusta, por cuanto contribuyen a consolidar el dictamen pericial con destino al juez o al jurado ante la corte o el tribunal para su veredicto que absuelva o condene al victimario

Como conclusión, la utilización de la auditoria forense aplicada a la tecnología y en el caso de la informática donde se realicen investigaciones criminales o financieras en la tecnología informática, esta proporciona una sólida base de evidencias físicas o los elementos materiales probatorios – EMP o las pruebas judiciales digitales relacionadas con un el caso o incidente o fraude o delito que se investiga, como con su análisis técnico especializado y apoyo en investigaciones y procesos legales. Su contribución puede ayudar a esclarecer los indicios de fraudes o de delitos o de incidentes que se presenten en las entidades o en las organizaciones empresariales, donde se identifica a los responsables o victimarios que lo cometieron, ayudando a

fortalecer controles internos y externos en futuros incidentes y el fortalecer la seguridad en el entorno tecnológico con base a los informes o dictámenes forense.