ISSN: 0798-1015 DOI: 10.48082/espacios-a20v41n42p32

REVISTA ESPACIOS

Vol. 41 (42) 2020 • Art. 32 • Especial COVID-19

Recibido/Received: 15/10/2020 • **Aprobado**/Approved: 31/10/2020 • **Publicado**/Published: 05/11/2020

Informática forense y auditoría forense: Nuevas perspectivas en tiempos de COVID-19

Forensic Informatics and Forensic Audit: New Perspectives in COVID-19 Times

MUÑOZ, Helmer[1]
CANABAL, Javier Dario[2]
GALINDO, Saúl Gonzalo[3]
ZAFRA, Brandon Steven[4]
BENÍTEZ, Yanh Jesús[5]

Resumen
La presente investigación muestra aspectos relacionados con la informática forense y la auditoría forense como perspectivas novedosas en tiempos de COVID-19, ya que son herramienta que permiten hacer una búsqueda especializada por medio de un peritaje a las organizaciones que lo solicitan, creando seguridad en las empresas. Se busca concientizar y generar cultura en las personas sobre la importancia de aplicar buenas prácticas en la seguridad informática ya que los riesgos informáticos son amenazas y vulnerabilidades que afectan en todos los aspectos a la empresa.
Palabras clave: informática forense, auditoría forense, riesgos informáticos, evidencia, vulnerabilidad.

Abstract
The present investigation shows aspects related to computer forensics and forensic auditing as novel perspectives in times of COVID-19 since they are a tool that allows organizations that request it to be carried out by means of an expert opinion, creating security in companies. It seeks to raise awareness and generate culture in people about the importance of applying good practices in computer security since computer risks are threats and vulnerabilities that affect the company in all aspects.
Keywords: forensic informatics, forensic auditing, computer risks, evidence, vulnerability.

1. Introducción

Hoy en día para afrontar los desafíos del COVID-19, todas las compañías, tanto públicas como privadas, al igual que las personas dependen de un factor muy importante “la tecnología”, ya que facilita que se puedan llevar a cabo todos los objetivos de un negocio, además, esta es una herramienta que sirve para realizar intercambio de

[1] Docente Investigador. Programa Contaduría Pública. Universidad del Sinú. Ingeniero de Sistemas. MsC en Ingeniería de Control Industral. PhD en Gerencia. Postdoctor en Procesos Sintagmáticos de la Ciencia y la Investigación. helmermunoz@unisinu.edu.co
[2] Docente Investigador. Programa Contaduría Pública. Universidad del Sinú. Administrador de Empresas. MsC en Gestión de Organizaciones. PhD en Educación. Postdoctor en Procesos Sintagmáticos de la Ciencia y la Investigación. javiercanabal@unisinu.edu.co
[3] Docente Investigador. Programa Contaduría Pública. Universidad del Sinú. Abogado. Contador Público. Msc en Ciencias de la Educación. PhD en Educación con Especialización en Mediación Pedagógica. saulgalindo@unisinu.edu.co
[4] Joven Investigador. Programa Contaduría Pública. Universidad del Sinú. brandonzafra@unisinu.edu.co
[5] Docente invsetigador ONCTI. Observatorio Nacional de Ciencia y Tecnología. Programa de Estimulo a la Innovación e Investigación, PEII. Licenciado en Educación Integral. Especialista en Planificación y Evaluación de la Educación. Doctor en Ciencias de la Educación. Postdoctor en Procesos Sintagmáticos de la Ciencia y la Investigación. yanhje49colombia@gmail.com

información y para poder desarrollar actividades de la vida diaria. No obstante, las informaciones que se registran en una compañía de todos los procesos que se realizan dentro de los equipos electrónicos a las vez van generando como especie de un archivo digital, la misma que tiene gran importancia por lo relevante de su contenido pues las estrategias de las empresas pueden ser proyectadas en base a esta información, de allí que podemos considerarla como el activo más importante de las empresas.

Sin embargo, es importante saber que aparte de la información, hay otros activos con los que cuenta una compañía, como los computadores, teléfonos, correos electrónicos, discos duros, entre otros., los cuales son un blanco directo para los ciberdelincuentes que solo están esperando el momento adecuado para atacar, es por ello que se deben tomar ciertas medidas que ayuden a prever que se presenten dichos acontecimientos, por lo que se debe tener un control riguroso sobre los medios en los que se interactúan en la organización.

Día a día las empresas compiten internacionalmente por el financiamiento necesario para llevar a cabo sus estrategias de inversión como consecuencia de la globalización financiera y las nuevas tecnologías de información. Ello ha conducido a mercados financieros complejos y sofisticados. (Pérez-Iñigo & Ferrer, 2015)

Por consiguiente, el uso de las redes y la innovación tecnológica, han hecho que la informática forense como herramienta para afrontar el covid 19 tome un valor muy importante en las organizaciones, ya que la información que se encuentra almacenada es vulnerable, y puede estar expuesta a manipulaciones, por este motivo debe ser resguardada a través de una adecuada gestión de riesgos informáticos, en la cual se vea involucrada el compromiso de todas las personas que laboran en la empresa, con el fin de prever acontecimientos que lleguen a involucrar pérdidas económicas y llegue a estar expuesta la reputación de esta, por la fuga, robo u ocultamiento de información. Para prever estos tipos de riesgos o acontecimientos antes mencionados, las organizaciones deben implementar e invertir en distintos mecanismos de seguridad que ayuden a detectar a tiempo este tipo de hechos, creando planes estratégicos informáticos e incentivando la cultura en seguridad informática en todos los empleados, para que así se puedan mitigar estos riesgos.

Además, es importante destacar que la auditoríaa forense en esta época de pandemia por el coronavirus entra a ayudar a la informática forense como una herramienta alternativa para combatir la corrupción enfocada en hacer una revisión especializada a cargo de un perito para que se encargue de detectar los fraudes que se presentan con respecto a la malversación de fondos, filtración de la información, manipulación en los registros contables de la compañía, enriquecimiento ilícito, cohecho, soborno, desfalco, conflicto de intereses, entre otros, usando la auditoría forense como herramienta de detección, pero, este debe ser una persona que no haya tenido ningún tipo de relación con la entidad, para que de esta manera el proceso que se vaya a realizar sea más efectivo, puesto que no estaría involucrando sus intereses personales. Cuando se habla de peritos se hace referencia a que “no toda investigación realizada por peritos o expertos es exclusivamente delictiva, muchas veces, se limita a la comprobación de hechos con fines comerciales, contables financieros o simplemente administrativos (como en el caso de las auditorías, contables, financieras, etc.)”.(Darahuge & Arellano, 2011, p. 28)

Generalmente en las organizaciones se presentan problemas financieros que resultan difíciles de manejar; enfrentar los costos financieros, el riesgo, baja rentabilidad, conflictos para financiarse con recursos propios y permanentes, toma de decisiones de inversión poco efectivas, control de las operaciones, reparto de dividendos, entre otros. Una empresa que enfrente un entorno difícil y convulsionado con los inconvenientes descritos anteriormente, debe implementar medidas que le permitan ser más competitiva y eficiente desde la perspectiva económica y financiera, de forma tal que haga mejor uso de sus recursos para obtener mayor productividad y mejores resultados con menores costos; razón que implica la necesidad de realizar un análisis exhaustivo de la situación económica y financiera de la actividad que lleva a cabo. (Nava, 2009)

La prueba documental ha sido desde la invención de la escritura, el principal aliado de la investigación judicial. Actúa como respaldo de la mayoría de los procesos. Ni siquiera la oralidad procedimental la ha podido desplazar, el documento forma parte de nuestra forma de ser y de nuestra sociedad, podemos "despapelizar" los procedimientos, pero no prescindir de los documentos soportados en papel. (Darahuge & Arellano, 2011, p. 33), ya que a través de estas pruebas se ha podido demostrar ante un juez la veracidad y autenticidad de los hechos, por lo que se consideran importantes dentro de un proceso judicial, puesto que al momento de una persona alegar, tenga con que defenderse.

Por consiguiente, en el desarrollo de esta investigación se tratarán temas como la informática forense, su definición, luego se hablara sobre sus inicios, seguidamente sobre los objetivos de la informática forense, la auditoría forense y la importancia que tienen así como las nuevas perspectivas en tiempos de COVID- 2019, además de identificar cuales son aquellos activos con los que cuenta una compañía, y finalmente, se hablará sobre las herramientas y usos que son utilizadas en la informática forense para esclarecer "el crimen" de los delitos informáticos. y finalmente, se hablará de COVID-2019 como pandemia actual y su impacto en las áres de informática forense y auditoría forense.

2. Aspectos teóricos

2.1. ¿Qué es la informática forense?

La informática forense ha sido descrita como el análisis de datos digitales o ha sido vinculada a los medios criminalísticas, pero siendo claros y concisos, una manera muy sencilla de definir este concepto es como un proceso metodológico en el cual se realizan una serie de procedimientos con el fin de recoger evidencias de datos digitales de un sistema de dispositivos de forma que pueda ser analizado y examinado por personas expertas.

Algunos autores como Castillo, & Bohada (2015) la definen como la ciencia que permite la adquisición, preservación, recuperación y presentación de los datos que son procesados de manera electrónica y guardados en soportes informáticos.

Según Zuccardi & Gutiérrez (2015) la informática forense fue creada por la Oficina Federal de Investigación de los Estados Unidos (FBI), con el propósito de velar por las necesidades específicas y articuladas de aplicación de la ley, a través de la realización de pruebas electrónicas.

Por su parte, Guevara (2018) la define como una ciencia del área de la computación que ha surgido recientemente debido a la necesidad de entender los acontecimientos ocurridos durante un evento o incidente relacionado con la seguridad informática en el cual ésta ha sido vulnerada por un atacante con el fin de afectar a dicho sistema ya sea modificando , destruyendo, o robando la información, por mencionar algunas acciones que pueden afectar la integridad, confidencialidad o disponibilidad de un sistema, o el conjunto de ellos".

En relación con estos conceptos y como se expuso inicialmente la informática forense no es más que una ciencia que ayuda a recuperar aquellos datos que han sido procesados digitalmente, esta se encarga también de colaborarle a la justicia, puesto que, a través de la obtención de evidencia, facilita los procesos en los tribunales con el fin de analizar, construir y realizar cualquier tipo de investigaciones.

No obstante, la informática forense se dice que inició en la década de los 80 cuando los computadores personales empezaron a tomar forma, es decir, cuando empezó una gran demanda por parte de los consumidores.

A comienzo de los años 90, la Federal Bureau of Investigación (FBI), observó que las pruebas o evidencias digitales tenían el potencial de convertirse en un elemento de prueba tan poderoso para la lucha contra la delincuencia, como lo era el de la identificación por ADN. Para ello, mantuvo reuniones en su ámbito, y a finales de los años

90 se creó la International Organización of Computer Evidence (IOCE) con la intención de compartir información sobre las prácticas de informática forense en todo el mundo. (Rodríguez & Doménech, 2011)

El G8 (Grupo de los Ocho), es un grupo de países industrializados del mundo cuyo peso político, económico y militar es muy relevante a escala global, integrados por Alemania, Canadá y Estados Unidos, en marzo de 1998 encargó a la OICE a través del grupo de Lyon el desarrollo de una serie de principios aplicables a los procedimientos para actuaciones sobre pruebas digitales, así como la armonización de métodos y procedimientos entre las naciones que garantizasen la fiabilidad en el uso de las pruebas digitales recogidas por un estado para ser utilizadas en tribunales de justicia de otro estado. (Rodríguez & Doménech, 2011)

Esto da a entender que las potencias mundiales encontraron un método para poder acabar con el fraude informático ocasionado en las empresas importantes de estas potencias y un nuevo paso para poder confiar plenamente en el uso de las tecnologías en todos los ámbitos.

Gracias a los buenos resultados que trajo consigo la informática forense, a mediados del 2001 esta fue puesta en marcha en Latinoamérica, siendo este un momento donde países latinoamericanos surgían como posibles futuras potencias, hacia el punto que esta novedosa metodología llegara, iniciando en México con una empresa llamada Mattica, la cual fue un laboratorio de investigación en delitos informáticos con un objetivo específico el cual es brindar a personas, empresas y organizaciones, privadas y gubernamentales, un servicio de investigación digital seguro y confiable con los estándares más rigurosos de calidad y confidencialidad, y gracias a esto, es posicionada con el primer laboratorio de informática forense que se encuentra a la par que otros laboratorios de países líderes en este tema. Este tiene como finalidad la identificación, análisis y preservación de pruebas derivadas de incidentes informáticos para la presentación de pruebas en procesos legales.

Y no solo se encuentra en México, en Colombia hace 11 años, Mattica fue instaurada, esta llega en un momento crucial en la historia de Colombia, debido a que se presentan muchos fraudes informáticos y todos eran ignorantes o no conocían sobre esto. El robo de información por los ciberdeliencuentes suponía un gran problema tanto para organizaciones como para las personas del común pero un año después de ser instaurado este laboratorio, la informática forense es apoyada en el marco legal por la ley 1273 del 2009 llamada también “ley de la protección de la información y de los datos”, que trata sobre la protección de organizaciones o gente del común de los ataques generados por terceros, siendo estos ataques, el manejo de sus datos personales, llevando a esto como un delito, es por eso que hoy en día la informática forense está tomando gran importancia en las empresas como una herramienta de gestión de la información, ya que a través del uso de las Tecnologías de la Información y la Comunicación (TIC), se pueden llegar a resolver casos sobre los múltiples delitos informáticos que se presentan a diario en las compañías.

Por otro lado, la informática forense tiene 3 objetivos, a saber:

1. La compensación de los daños causados por los criminales o intrusos.

2. La persecución y procesamiento judicial de los criminales.

3. La creación y aplicación de medidas para prevenir casos similares.

Estos objetivos son logrados de varias formas, entre ellas, la principal es la recolección de evidencia. (López, Amaya, León, & Acosta, 2001)

La obtención de evidencia al aplicar la informática forense es el elemento clave para soportar, conocer y analizar los hechos en los cuales la información de las empresas se ven en peligro ante al sufrimiento de ataques cibernéticos en sectores como el financiero donde constantemente se mueven cantidades de dinero, otro sector

puede ser el de comercio electrónico, partiendo de que hoy en día se realizan pagos online donde se debe suministrar una serie de datos personales que pueden llegar a ser manipulados por personas ajenas.

Sin embargo, muchos casos se han presenciado sobre el robo de la información financiera, debido a que es la más apetecida por los delincuentes, que lo que buscan es obtener dicha información y manipularla a su favor, perjudicando la economía y estabilidad de las organizaciones afectadas; por su parte, cada uno de estos objetivos traen consigo una finalidad, el primero hace referencia a que los investigadores se basan en las pruebas para contrarrestar o compensar los daños ocasionados, el segundo establece el seguimiento de los delincuentes que cometieron el delito, y el tercero es la de crear barreras que impidan el surgimiento de estas acciones nuevamente, para minimizar el robo de información.

La recolección de evidencia es fundamental dentro de cualquier investigación, puesto que requiere de cuidados, ya que es aquí donde se deben proteger los equipos y toda la información que en ellos esta suministrada, debido a que en ocasiones estas pueden llegar a ser violentadas.

En la parte contable, respecto a la auditoría forense, se puede obtener evidencia acerca de sucesos irregulares que hagan los mismos miembros de las empresas o en los casos donde se ve presenciado algún ataque cibernético, ya que si se hace una analogía, la auditoría forense busca realizar un estudio exhaustivo, es decir, ir más allá acerca de procesos que lleven a cabo las empresas en el ámbito contable, y de la mano de la informática forense, también puede estar capacitada para buscar información, causas y consecuencias de hechos que han sucedido dentro de estas respecto a robos de información mediante medios digitales.

Con respecto a las líneas de investigación en contabilidad estas son principalmente las siguientes: Control contable: Comprende el desarrollo de proyectos en el área de sistemas de información contable, contabilidad y planeación tributaria, costos, contabilidad y planeación estratégica, gestión social y ambiental, análisis de las declaraciones contables, presupuesto empresarial y auditoría operacional, conduciendo las investigaciones hacia las necesidades de la gestión económica, financiera y social de las organizaciones, en la búsqueda de controles y aportes para la racionalidad y eficacia de los negocios. (Saavedra & Saavedra, 2015)

2.2. Importancia de la auditoría forense dentro de la informática forense

La informática forense hace su aparición como una disciplina auxiliar de la justicia moderna, para enfrentar los desafíos y las técnicas de los intrusos informáticos, así como garante de la verdad alrededor de la evidencia digital que se pudiese aportar en un proceso (Cano, 2006).

Es decir, que esta disciplina surgió como una necesidad para aliarse con la justicia con el fin de ofrecer una aplicación de métodos y estrategias que puedan brindar soluciones a procesos legales; es por esto que esta definición no está muy alejada de lo que es la auditoría forense, pues, esta no es más que una auditoría especializada, la cual es utilizada como un instrumento o una herramienta con la que se obtienen evidencias sobre una investigación, que pasa por un proceso de verificación, para posteriormente convertirlas en pruebas.

“Entre estas ciencias forenses ha aparecido una nueva disciplina, proveniente de la informática, pero con sustento científico clásico, metodológico criminalístico y probatorio judicial.”

A esto se refiere a la informática forense que junto con la auditoría forense a través de la criminalística, que es “la disciplina que se encarga de brindar soporte a la investigación judicial. Se inicia aportando criterios científicos, tecnológicos y técnicos al análisis a posteriori de los hechos criminales, se orienta al derecho penal”, emplean metodologías como herramientas con el fin de llegar “a la verdad histórica o material del hecho” (Darahuge & Arellano, 2011, p. 11), es decir, se basa en lo que ha sucedido, para analizarlo y estudiarlo y llegar a la fuente que originó tal suceso. Es entonces, cuando se origina la relación entre estos dos términos forenses, que llevan su

objetivo alineado a la investigación y obtención de pruebas con una verificación especializada en la cual se puedan basar las conclusiones y en su defecto las decisiones en caso de tener que tomar alguna.

Además, estos dos términos tienen una relación puesto que ninguno de ellos es utilizado para prever los delitos informáticos, ya que para esta función específica esta la seguridad informática, que se define como la disciplina que se ocupa de diseñar normas, procedimientos o métodos y técnicas destinadas a conseguir un sistema de información seguro y confiable (Aguilera, 2011).

En otras palabras, es aquella que está encargada de la protección de los datos y del mal uso que se les dé a estos, por esta razón, si existe un mal control en la seguridad de la información, es cuando surgen los delitos informáticos y a raíz de estos se utilizan herramientas como la informática y auditoría forense para poder detectarlos con base a indagaciones avanzadas y darles una solución.

Por estas razones es de mucha importancia la auditoría forense en los procesos que lleve a cabo a la informática forense, ya que la auditoría forense se encarga de instrumentar por medio de herramientas de una investigación científica un análisis, documentación e identificación de pruebas que pueden fortalecer y fortificar las investigaciones que lleve a cabo la informática forense, ya que ambas trabajan bajo un proceso de esclarecimiento de la información y de la realidad en la que se encuentre la empresa. Asimismo la búsqueda de alternativas y soluciones sobre las repercusiones que traiga consigo al ente económico.

Sin embargo, en el área contable se llevan muchos procesos que son de fundamental importancia y de mucho cuidado, aunque se presentan casos donde los empleados, o los mismos miembros no realizan de manera correcta sus labores y por ende tienden a manipular la información que están manejando; es por ello que existe la figura de un auditor en las empresas, ya sea interno o externo, para regular estas situaciones y detectar y prevenir sucesos en contra de ley, pero un auditor externo es más efectivo debido a que no ha tenido contacto alguno con la empresa.

Con ayuda de un auditor, expertos en informática forense, pueden aliarse para realizar un trabajo minucioso de lo que se hace a diario en una empresa, y no solo se podría iniciar investigaciones o la búsqueda de algo ilegal realizado por los miembros de la organización, sino que también para llevar a cabo un estudio acerca de sucesos que perjudicaron o están perjudicando a las empresas, en el tema de robo de información.

Es decir, estas dos fuentes de investigaciones exhaustivas pueden también indagar sobre actos delictivos que han cometido personas ajenas a las empresas con el propósito de robarle la información de todos los movimientos que realizan. “La informática forense y la auditoría informática o contable, al respecto esta última tiene fines de supervisión sobre la gestión de los activos informáticos de una persona física o jurídica, aunque en general se refiere a esta última en el formato de empresas de muy diversa índole. Si bien la informática forense actúa en soporte de dicha auditoría, esta trasciende a la primera, ya que las herramientas informático-forenses brindarán los elementos necesarios para su ejecución práctica, pero no aportarán datos referidos a la legalidad o legitimidad de los resultados obtenidos”. (Darahuge & Arellano, 2011, p. 22)

Teniendo en cuenta que en una organización se maneja mucha información importante y confidencial, dentro de los activos principales que son utilizados como material de investigación se encuentran dispositivos electrónicos como: teléfono celular, computadores, correos electrónicos, páginas web, discos duros, entre otros. Además de equipos informáticos que permiten la obtención de registros y datos con el fin de ser utilizados como medios de prueba ante los tribunales.

Una de las formas de cómo se pueden llegar a evidenciar este tipo de delitos informáticos, puede ser mediante la suplantación de identidades, es decir, cuando personas se hacen pasar por trabajadores de la empresa para ponerse en contacto con alguno de los departamentos que tiene la organización (RRHH, Contabilidad, Tesorería,

entre otros.) los cuales son apetecibles por los delincuentes, en qué sentido, a través de llamadas pueden ponerse en contacto con algunos de los departamentos, en este caso RRHH y pedir el cambio de su cuenta bancaria, esto con el fin de que el pago de la nómina no le llegue a la persona que corresponde sino a aquella que está suplantando la identidad, y cómo se puede caer fácilmente en esto, cuando la cuenta del remitente ha sido comprometida, esta técnica es conocida como email spoofing y se basa en la suplantación de identidad del remitente.

Email spoofing, es un término utilizado para describir (generalmente fraudulenta) la actividad de correo electrónico en la que la dirección del remitente y otras partes del encabezado del correo electrónico se modifican para que parezca que el correo electrónico se originó de una fuente diferente. (Pandove, Jindal, & Kumar, 2010)

Es decir, cuando en la organización se manejan correos electrónicos de la misma índole tanto para trabajadores como para la parte gerencial, en la cual la persona que recibe la información no se da cuenta de la diferencia, por lo tanto, es muy importante que se revisen los correos electrónicos, los números de llamadas y ante las dudas se pida información más exacta que corrobore si se está tratando con la persona correcta y no con algún intruso.

Por lo que no es recomendable quedarse únicamente con la información que proporcionan o suministran los equipos o las personas, es importante también ir al lugar donde ocurrieron los hechos para poder esclarecer de manera más eficiente y coordinada todo lo ocurrido en la organización.

Si estos dispositivos son alterados los investigadores deben revisar que al momento de hacer la copia del disco original esta no esté violentada, puesto que, de ser así la evidencia que se tendría no serviría para nada, ya que se debe tomar la información sin necesidad de ocasionar daño alguno en ellos.

Según Castillo & Bohada (2015) existen una serie de procedimientos o herramientas que nos permiten extraer la información sin tener que por algún motivo alterarla, manteniendo así la cadena de custodia de los dispositivos, partiendo de que se debe preservar la evidencia digital, dentro de las herramientas se encuentran las siguientes:

Disco y captura de datos: se encargan de proteger o reparar el disco duro mediante limpiezas, optimización de espacio, verificación de la integridad del sistema lógico, entre otros.

Dentro de estas herramientas se encuentran:

• Recovers: Esta herramienta se encarga de recuperar las URL de acceso a sitios web y ficheros correspondientes, que en algún momento fueron eliminados.

• Pandora Recovery: Recupera la mayor parte de información de un disco formateado o los archivos eliminados del dispositivo electrónico.

• Open Freely: Permite realizar la visualización y edición de un archivo en cualquier formato y brinda las características técnicas del archivo.

• Visores de archivos Free Opener: Esta herramienta brinda la opción de visualizar diferentes formatos de archivos, tales como imágenes, texto, música, video audio.

Análisis de Registro. Permiten obtener información de todos los datos relacionados en el registro que se generan en los computadores cuando se tiene instalado un sistema operativo Windows.

Podemos mencionar algunas de estas herramientas:

• Regripper registry decoder: Estas herramientas permiten realizar la extracción y correlación de la información de los registros, mostrando al final un listado detallado de dicha información.

• MUI Cacheview: Permite al usuario visualizar y corregir la información relacionada al nombre de las aplicaciones que se están ejecutando.

• Recon Registro: Permite obtener información de los registros del sistema que se han eliminado sin importar el tiempo que haya transcurrido.

Análisis de Correo Electrónico: este es uno de los medios en los que más se pueden llegar a cometer delitos informáticos, puesto que existen herramientas capaces de buscar los correos ya eliminados o alterados hasta dar con el original.

Dentro de estas herramientas se encuentran:

• FTK (Forensic Toolkit): herramienta de uso comercial, soporta servidores de correo electrónico, tales como Outlook (PST), Outlook Expres (DBX), Netscape, Yahoo, MSN.

• Eindeuting: esta herramienta es open source y soporta servidores de correo electrónico, tales como Outlook (PST), Outlook Expres (DBX).

Forenses de Red: se encarga de encontrar patrones anómalos conexiones sospechosas, basadas en el tráfico de datos.

Algunas herramientas son:

• Wireshark: permite capturar paquetes de la red, analizando conexión y detectando posibles problemas en la transmisión de paquetes, y presentando el resultado del análisis mediante una interfaz gráfica.

• Xplico: extrae todo el contenido de datos de una red, como por ejemplo información de correo electrónico como protocolos, todos los contenidos HTTP, información de llamadas VoIP, entre otras.

Análisis de Dispositivos Móviles: Al igual que el correo electrónico, los dispositivos móviles se encuentran inmerso a los delitos informáticos, ya que es muy fácil extraer información de ellos.

Algunas herramientas son:

• Oxígeno Suite Forense: obtiene todo tipo de información eliminada, dañada o manipulada (registro de llamadas hechas o recibidas, mensajes de texto, correos electrónicos, contactos, documentos).

• XRY: fue diseñada para recuperar todo tipo de información que se encuentre en el dispositivo móvil, así como las características del mismo, viene con un dispositivo para hardware y para software.

Adquisición y Análisis de Memoria: adquiere la información que se almacena en la memoria RAM.

Las herramientas son:

• Responder CE: esta herramienta permite capturar la memoria RAM, para su posterior análisis.

• Volatility: se encarga de realizarle un seguimiento a los procesos indicados por el especialista forense, con el fin de extraer información útil para su posterior análisis.

Recuperación de Contraseñas: esta es una de las más usadas por los investigadores forenses para poder ingresar a cualquier dispositivo.

Algunas herramientas son:

• Ntpwedit: sobrescriben la contraseña de un usuario o un administrador, y así poder iniciar sesión con la información editada, estas herramientas son limitadas, ya que solo aplican para los sistemas basados en Windows NT (como Windows 2000, XP, Vista, 7 y 8).

• Mail PassView: recupera contraseñas de cuentas de correos electrónicos.

Estas herramientas, ayudan a los investigadores de alguna manera a facilitarle los trabajos, puesto que cada uno cuenta con funciones específicas, lo que hace que los peritos forenses puedan estudiar de manera detallada cualquier dispositivo digital dependiendo de la necesidad que se requiera en ese momento. Teniendo en cuenta que las empresas basan su actividad en los sistemas de información, a través de los nuevos soportes tecnológicos. No obstante, el uso constante de estos sistemas hace que las empresas se conviertan en el objetivo de los ciberdelincuentes, ya que se aprovechan de las vulnerabilidades que tienen estos para poder acceder y así desarrollar su actividad delictiva.

Por consiguiente, es importante utilizar diferentes medios para asegurar, guardar, y procesar la información, debido a que, así como pueden llegar a surgir muchas herramientas que ayuden a combatir que alteren o eliminen la información, habrá miles que persigan lo contrario.

Sin embargo, se requiere que los dueños de las organizaciones busquen implementar una infraestructura tecnológica basada en una cultura de buenas prácticas de la informática y la información, puesto que muchas empresas no disponen de una infraestructura tecnológica interna, sino que lo hacen por medio de un outsourcing, es decir, empresas externas que se encarguen del manejo de estas.

Por otra parte, según López, Amaya, León, & Acosta (2001), dentro de la informática forense, existen una serie de usos que permiten recolectar información y que guardan estrecha relación con la vida cotidiana. A continuación se mencionan cada uno de ellos:

1. Prosecución Criminal: Evidencia incriminatoria puede ser usada para procesar una variedad de crímenes, incluyendo homicidios, fraude financiero, tráfico y venta de drogas, evasión de impuestos o pornografía infantil.

2. Litigación Civil: Casos que tratan con fraude, discriminación, acoso, divorcio, pueden ser ayudados por la informática forense.

3. Investigación de Seguros: La evidencia encontrada en computadores, puede ayudar a las compañías de seguros a disminuir los costos de los reclamos por accidentes y compensaciones.

4.Temas corporativos: Puede ser recolectada información en casos que tratan sobre acoso sexual, robo, mal uso o apropiación de información confidencial o propietaria, o aún de espionaje industrial.

5. Mantenimiento de la ley: La informática forense puede ser usada en la búsqueda inicial de órdenes judiciales, así como en la búsqueda de información una vez se tiene la orden judicial para hacer la búsqueda exhaustiva.

Cada uno de estos usos se convierte en un conjunto de herramientas o alternativas para recopilar pruebas documentadas o medios probatorios que soporten las indagaciones que se encuentra en una investigación forense, aplicando una serie de técnicas como la observación, inspección e indagación entre otros que faciliten identificar los delitos.

2.3. Informática forense y auditoría forense: Nuevas perspectivas en tiempos de COVID-2019

La humanidad se vio totalmente sorprendida por un nuevo virus de infección respiratoria aguda SARS-CoV-2 perteneciente a la familia del coronavirus recientemente descubierto, cuya mutación se propaga rápidamente

por todos los países del mundo, afectando directamente a personas, instituciones, organizaciones, empresas, y causando un desequilibrio imperante en los aspectos sociales, políticos, culturales, pero sobremanera en el aspecto económico de cualquier entidad.

Es un hecho que la crisis exponencial derivada del Coronavirus del año 2019, también denominado COVID-19 ha ocasionado diversos impactos significativos y trascendentales en el funcionamiento de los estados financieros de la empresa y el control de sus registros contables, lo que a su vez ha generado pérdidas económicas masivas y diversos riesgos informáticos que amenazan la seguridad, productividad y competitividad de la misma.

Asimismo, los efectos del COVID-19 han propiciado la caída abrupta del valor de las acciones de las empresas, los presupuestos, los costos, el comercio y sus activos. Las ventas y los ingresos de igual modo se han visto afectados por las medidas de protección llevadas a cabo para contrarrestar la propagación del virus.

Otros factores que se han visto obstaculizados por la presencia del COVID-19 son el aumento de la producción, la celeridad de suministros, la completa disposición por parte del personal que labora en las empresas, las ganancias, los niveles de demanda, el financiamiento, el flujo continuo de efectivo, los viajes, los proyectos de inversión, las actividades realizadas en los diversos contextos de la sociedad, entre otros.

En este sentido, se puede afirmar que el coronavirus ha propiciado un impacto global de carácter negativo en los mercados financieros de los diferentes países, y por ende en la economía mundial.

En el caso de la presente investigación, es importante mencionar que la situación actual enmarcada por la pandemia del coronavirus 2019, ha generado un fuerte impacto en las áreas de informática y auditoría forense, debido a que se ha visto afectada en gran medida la seguridad digital e informática de las empresas, lo que a su vez evidencia la vulnerabilidad de sus políticas de seguridad y la falta de protección tanto de la información como de las tecnologías para la gestión de información.

Un ejemplo que también evidencia lo planteado, es lo relacionado con los delitos informáticos y fraudes electrónicos cometidos por los Hacker, como ciberdelincuentes que aprovechan el contexto del COVID-19 para cometer tales violaciones que quebrantan la seguridad empresarial. Esto generan canales de comunicación con ataques cibernéticos para traficar datos e informaciones de manera ilícita.

Uno de estos principales ataques es el phishing, medio a través del cual se le envía correos a los directores y empleados de las empresas ofreciéndole beneficios para combatir el coronavirus, donde le piden que sigan las instrucciones para descargar un archivo que contiene un software malicioso conocido como “malware”, el cual genera daños en los sistemas, y toma control de la información acumulada en las máquinas.

Otra sitios que usan los ciberdelincuentes son las páginas web maliciosas, es decir, páginas falsificadas que contienen información sobre la propagación de la pandemia, mediante las cuales se instalan dispositivos que posibilitan el robo de información de las computadoras. Otras se hacen pasar por instituciones bancarias y modalidades de teletrabajo, que hacen confundir al usuario y les permite caer en la trampa. Y finalmente, existe la creación de sitios maliciosos creados como tiendas on line que venden items, mascarillas, e insumos médicos como medidas de protección para combatir el COVID-19, y otros que aceptan donaciones para tal fin.

Colombia no escapa a esta realidad, debido a que el coronavirus ha ocasionado un impacto negativo en la ciberseguridad de las empresas del país. En atención a las cifras más recientes publicadas por el Centro Cibernético de la Policía Nacional, los delitos informáticos aumentaron un 59% en el primer semestre, respecto al mismo periodo del año pasado, motivado a que la pandemia estimuló en los colombianos el uso de las operaciones digitales.

Por ejemplo, en lo que va de pandemia se han registrado más de 17.211 denuncias, y 2.103 casos de suplantación de sitios web, un delito que creció en 364%.

En relación con este nuevo contexto en el país, un reciente estudio de TransUnion, que incluye a Colombia, evidenció que el 'phishing' es el principal medio de fraude digital en todo el mundo. De acuerdo con el documento, el 27% de los consumidores encuestados manifestaron haber sido víctimas de este tipo de estafa con temas vinculados con la pandemia.

De igual modo, un 21% de los estudiados precisó haber sido víctima de estafas de terceros originados mediante enlaces desde sitios web legítimos de comercio en línea, mientras que un 19% indicó que fue estafado a través de supuestos fondos de recaudación para caridad.

Todos estos hechos y datos reflejados, son evidencias claras del fuerte impacto que ha provocado la pandemia en la áreas de informática y auditoría forense, en términos de seguridad de la información empresarial.

Por tal motivo, en medio de estas problemáticas originadas por la crisis de la pandemia del COVID-19, es urgente disponer de una información contable confiable que involucre el aspecto económico, financiero, social, político, entre otros. He aquí donde juega un papel importante la contabilidad pues de trata de la ciencia que permite el estudio, el registro, la medición y el análisis exhaustivo de la situación económica financiera de la empresa, así como de su patrimonio, y la informática pues ésta última contribuye a optimizar las operaciones contables, y los documentos necesarios para realizar los informes financieros de manera más exacta, auténtica y rápida. Ambas ciencias se relacionan entre sí y son relevantes pues permiten afrontar los desafíos venideros en cualquier organización o empresa.

Ahora bien, desde el inicio del aislamiento preventivo derivado de la pandemia, han disminuido las operaciones en oficinas y sucursales de entidades financieras y han aumentado las transacciones en los canales no presenciales como banca móvil y los portales bancarios.

En este sentido, uno de los grandes desafíos que afronta la empresa en los momentos actuales es la seguridad de su información financiera. Por consiguiente, cabe preguntarse ¿Cómo hacer frente a esta pandemia mundial denominada COVID-19 para dar celeridad y seguridad a todos los procesos administrativos y contables en la empresa?

Ante tal situación, desde la presente investigación se propone la dualidad informática forense y autoría forense para mitigar los riesgos informáticos y de seguridad en las empresas causados por el accionar de los ciberdelincuentes en el contexto mundial. Por tal motivo, en tiempos de COVID es de suma importancia la denominada ciberseguridad, como proceso informático que permite disminuir los diferentes fraudes relacionados con la información financiera.

Por tal motivo, la informática forense y la auditoría forense deben ser vistas desde otra perspectiva, enfocada en el uso de herramientas tecnológicas especializadas e innovadoras que permitan contrarrestar los delitos informáticos ilegales que se derivan del uso inadecuado de las TIC por parte de los ciberdelincuentes. En este contexto, juega un papel fundamental la ciberseguridad, debido a que toda empresa para minimizar los riesgos asociados con la seguridad informática debe contar con dispostivos tecnológicos que permitan recopilar, analizar, evaluar y conservar evidencia digital de cualquier fraude electrónico que se cometa en la empresa.

Por ello, es muy importante que las empresas asuman estas perspectivas innovadoras relacionadas con la informática y la auditoría forense, sin violar las líneas de seguridad, para poder adaptarse a la situación y puedan continuar su producción.

De igual manera, tras esta crisis y las diferentes medidas adoptadas para combatir la pandemia, es pertinente evaluar la capacidad que tienen las organizaciones para funcionar de forma adecuada, en aras del futuro próximo.

Ante todo lo planteado, se debe entender que lo más importante para darle continuidad al funcionamiento de las empresas es la protección, la salud y el bienestar de los empleados, pues de ellos depende en gran medida el éxito de las actividades realizadas en dichas instituciones. En este contexto, la comunicación y la motivación también son dos factores fundamentales para mantener la seguridad de las organizaciones en todas sus aristas. En otras palabras, se trata de que las empresas busquen la protección de su fuerza laboral, sus operaciones, sus valores y sobretodo su información financiera y contable.

3. Conclusiones

Es evidente que el mayor uso de canales digitales y las restricciones a la movilidad han permitido situaciones simultáneas: disminución de fraudes en canales físicos como oficinas o cajeros respecto pero por el otro lado, se han presentado aumentos en los fraudes a través de medio virtuales. Es esí que en tiempos de COVID-19, la informática forense y la auditoría forense han adquirido gran relevancia en las empresas, ya que mediante los análisis informáticos que se realizan dentro de estas organizaciones se pueden llegar a descubrir cualquier tipo de ataque o fraude cibernético, considerando que los avances tecnológicos han hecho que la información se puede llegar a ver afectada por un sin número de manipulaciones como piratería de software, al hackeo de cuentas; así como también espionaje industrial, debido a las frecuentes transacciones que se realizan en una organización.

Ante lo expuesto, es muy importante que se concientice a los usuarios en el uso de las redes informáticas ya que el desconocimiento o la ignorancia por parte de los trabajadores al momento de su utilización puede llegar a generar vulnerabilidades, las mismas que son aprovechadas por los atacantes informáticos o ciberdelincuentes para tener accesos no autorizados, y robar información sensible, confidencial e importante de las organizaciones, por este motivo es importante que cuando los usuarios detecten cualquier anomalía que vean diferente a lo que con frecuencia realizan, la informen a tiempo porque pueden estar expuestas a muchos riesgos, si se deja pasar y no se avisa a las áreas encargadas.

Por consiguiente, cuando surgen delitos informáticos, aparece la informática forense, buscando extraer y recopilar datos que le sirvan para detectar el crimen, por eso se dice, que esta es una ciencia auxiliar de la justicia, puesto que, puede llegar a facilitarle las tareas a los tribunales, sin embargo, hay que tener en cuenta que esto se hace a través de un perito, y de ayuda alguna con la auditoría forense, siendo esta una herramienta especializada que busca a través de la obtención de evidencia suficiente y adecuada colaborar en la investigación, con el fin de que se pueda obtener una seguridad informática, y como se llega a esto, conociendo y sabiendo que hay que darle un buen uso a los dispositivos, además, de que en las organizaciones busquen que los empleados, reciban información constante y se capaciten en todo este mundo de la informática.

No obstante, la misma tecnología es la encargada de ofrecernos una variedad de dispositivos o herramientas para guardar, respaldar y proteger la información, la misma que nos servirá como prueba digital ante un hecho ocurrido.

Además, las empresas hoy en día deben contar con equipos profesionales tanto de software como hardware, que puedan realizar análisis y pruebas de seguridad de la información, los cuales permitan determinar la presencia de vulnerabilidades en los equipos informáticos y redes de datos, teniendo en cuenta que la única manera para mitigar y proteger la información es mediante una gestión de riesgos informáticos que forme parte de su plan estratégico empresarial.

4. Referencias bibliográficas

Aguilera, P. (2011). Redes seguras. (Seguridad informática). Madrid, España: Editex

Cano, J. (2006). Introducción a la informática forense. Revista Asociación Colombiana de Ing. de Sistemas (ACIS) (96), 64-73. Disponible en: http://www.acis.org.co/fileadmin/Revista_96/dos.pdf

Castillo, L. F., & Bohada, J. A. (2015). Informática Forense en Colombia. Ciencia, innovación y tecnología, 2, 83-94.

Darahuge, M. E., & Arellano González, L. E. (2011). Manual de informática forense Buenos Aires ERREPAR SA.

Foro de Seguridad (2019). http://www.forodeseguridad.com/artic/discipl/4166.htm

Guevara, E. (2018). Alcances que puede tener una investigación forense dentro de un proceso legal en Colombia. Universidad Nacional Abierta y a Distancia UNAD. Bogotá.

López, Ó., Amaya, H., León, R., & Acosta, B. (2001). Informática Forense: Generalidades, aspectos técnicos y herramientas. Universidad de los Andes. Colombia.

Nava, M. A. (2009). Análisis financiero: una herramienta clave para una gestión financiera eficiente. Revista Venezolana de Gerencia, 14(48), 606-628.

Pandove, K., Jindal, A., & Kumar, R. (2010). Suplantación de correo electrónico. Revista internacional de aplicaciones informáticas. Vol.5, Núm.1. Chandigarh.

Pérez-Iñigo, J. M., & Ferrer, M. A. (2015). Finanzas y contabilidad. Revista Venezolana de Gerencia, 20(71), 391-393.

Rodríguez., F., & Doménech, A. (2011). La informática forense: El rastro digital del crimen. Cuadernos de criminología: revista de criminología y ciencias forenses (14), 14-21.

Saavedra, M. L., & Saavedra, M. E. (2015). La investigación contable en Latinoamérica. Actualidad contable. Acomodar. Vol.18, Num.31. 99-121. Universidad de los Andes. Venezuela. Disponible en: http://www.redalyc.org/articulo.oa?id=25743363006

Zuccardi, G., & Gutiérrez, J. D. (2015). Informática Forense en Colombia. Ciencia, Innovación y Tecnología (RCIYT), II, 9. Disponible en: http://pegasus.javeriana.edu.co/~edigital/Docs/Informatica%20Forense/Informatica%20Forense%20v0.6.pdf