Riesgos presentes en los ciberataques: un análisis a partir de herramientas de auditoría forense

Resumen

La auditoría forense adquiere importancia con la evolución de los sistemas informáticos, debido al desarrollo de nuevos mecanismos utilizados por parte de las entidades para agilizar procesos organizacionales, presentando información confiable y oportuna a sus usuarios; de aquí que la auditoría forense se convierte en el instrumento que mejora los procesos existentes para detectar y prevenir operaciones sospechosas, encontrando los elementos necesarios para su mejoramiento. En el campo de los ciberataques, la auditoría forense debe encargarse de analizar las herramientas que revelen el delito analizando la gestión y el control interno de las entidades teniendo en cuenta el cumplimiento de las normas y procedimientos establecidos, en consecuencia de identificar y evaluar los riesgos presentes en los ciberataques. Por consiguiente, en el presente artículo de reflexión se realiza una metodología de estudio descriptivo y cualitativo, profundizando en el análisis de las herramientas de la auditoría forense que permitan la identificación y evaluación de los ciberataques. Los resultados del estudio evidencian que la auditoría forense procede en el control para las entidades vulnerables a los ciberataques, detectando los riesgos más relevantes que se analizan a partir de un caso práctico y presentando las herramientas esenciales para su evaluación y prevención.

Palabras clave: auditoría forense, información financiera, malware, operaciones sospechosas, riesgo reputacional.

Risks present in cyberattacks: an analysis from the tools of forensic audit

Abstract

Forensic audit becomes important and evolution of computer system, due to the development of new mechanisms used by the institutions to streamline organizational processes, presenting reliable and timely information to all users, from this point the forensic audit becomes an instrument that improves existing processes to detect and prevent suspicious transactions, finding the necessary elements for improvement. in the field of cyberattacks, forensic audit should be responsible for analyzing the tools that reveal the crime by analyzing the management and internal control of the entities taking into account compliance with the rules and procedures established, the result of identifying and evaluating the risks involved in cyberattacks therefore reflection in this article is made with a methodology descriptive and qualitative studio, This is deepened in analyzes tools of forensic authority allowing the identification and evaluation of cyberattacks, the results of the study show that the forensic audit to be in control as entities vulnerable to cyber-attacks by detecting the most relevant risks discussed starting a case study and also presenting the essential tools for the evaluation and prevention.

Key words: financial information, forensic audit, malicious software, suspicious transactions, reputational risk.

Recibido: 2 de abril de 2015.
Aceptado: 17 de junio de 2015.

Ludivia Hernández Aros

Magíster en Auditoría y Gestión Empresarial de la Universidad UNINI – Puerto Rico Especialista en Revisoría Fiscal y Control de Gestión de la Universidad Cooperativa de Colombia. Profesora Investigadora Facultad de Contaduría Pública Universidad Cooperativa de Colombia, Sede Ibagué, Colombia, Grupo de Investigación PLANAUDI. Correo electrónico: Ludivia.hernandez@campusucc.edu.co

Jennifer Andrea Cerquera Suárez

Estudiante de décimo semestre pregrado, Programa contaduría pública Universidad cooperativa de Colombia- sede Ibagué. Correo electrónico: jennifer.cerqueras@campusucc.edu.co

Johanna Andrea Vanegas Rodríguez

Estudiante de décimo semestre pregrado, Programa contaduría pública Universidad cooperativa de Colombia- sede Ibagué. Correo electrónico: johanna.vanegasr@campusucc.edu.co

Riesgos presentes en los ciberataques: un análisis a partir de herramientas de auditoría forense

Introducción

El crecimiento imparable de los medios informáticos, la ubicuidad que brindan para facilitar todos los procesos de interacción y organización de la información personal y empresarial, abre un gran mundo de posibilidades para que los delincuentes busquen formas de conseguir datos de vital importancia para los usuarios, como lo son el acceso a claves bancarias, correos electrónicos a causa de la instalación de software maliciosos en los computadores, celulares o cualquier otro dispositivo.

La auditoría forense es el otro lado de la medalla en la labor de prevenir y estudiar hechos de corrupción. Asimismo, como en el caso de una auditoría tradicional, la auditoría forense evalúa el cumplimiento de procesos administrativos, de gestión, financieros entre otros y su propósito consiste en establecer los parámetros recurrentes para conectar los procesos afectados hallando evidencia significativa, promoviendo las herramientas que minimicen los riesgos relevantes.

Del mismo modo, la auditoría forense aplicada a hechos ya ocurridos, se convierte en una medida de detección, desarrollando todos instrumentos necesarios para evitar que estos vuelvan a ocurrir; estos hacen parte de las herramientas de auditoría forense para la identificación y evaluación de los riesgos presentes en los ciberataques. Para investigación en ciberataques debe ser orientada a nivel financiero de una empresa, el gobierno, personas o cualquier organización que maneje recursos (Maldonado, 2003).

Por ende, se busca con las herramientas de auditoría forense evidencias que comprueben los innumerables delitos informáticos que afectan la calidad de vida de la humanidad. Las pruebas son el elemento más importante en el proceso, porque éstas serán presentadas para comprobar el delito. Las

diferentes investigaciones sobre ciberataques se realizan con el apoyo de todas las aplicaciones que aseguran la información, registros bancarios, información gubernamental, registros comerciales, bases de datos, entre otros (Dueñas, 2009).

Cuando en la ejecución de labores de auditoría (financiera, de gestión, informática, tributaria, ambiental, gubernamental), se detecta fraudes financieros significativos; y se deba (obligatorio) o desee (opcional) profundizar sobre ellos, se está incursionando en la denominada auditoría forense (Ayala, 2008).

Así mismo, contar con diferentes mecanismos de control y seguridad para salvaguardar los riesgos latentes, se ha convertido en un tema primordial para la auditoría forense en la seguridad personal y de las empresas garantizando la confidencialidad de la información; de manera que el propósito de este artículo es determinar las herramientas de auditoría forense para identificar y evaluar los riesgos presentes en los ciberataques.

En primera instancia se presentan el marco legal nacional e internacional que promueve el control en el manejo adecuado de la información que se encuentra en base de datos personales, financiera, crediticia, comercial, además de los mecanismos que se puede adoptar para la detección de delitos informáticos; se presentan las herramientas utilizadas en la auditoría forense con ayuda de computadora y algunos puntos de vista de diferentes autores que han trabajado el tema. A continuación, se esbozan los resultados que generan las herramientas de la auditoría forense en la identificación y evaluación de los riesgos presentes en los ciberataques, para finalmente, presentar algunas conclusiones que sintetizan en forma general lo expuesto en los apartados anteriores.

Problema de investigación

La auditoría forense investiga y analiza los hechos relevantes al momento de generarse un fraude con el fin de salvaguardar los riesgos en los cuales incurren las personas o entidades; igualmente ayuda a la prevención y detección de estos a través de herramientas sistémicas, que permiten evaluar los problemas más comunes en las estafas presentadas en los ciberataques.

Por lo anterior, se debe conocer como actuar frente a las diferentes situaciones que se puedan presentar en una entidad y conocer las herramientas de la auditoría forense para la identificación y evaluación de los riesgos presentes en las estafas comunes de los ciberataques financieros.

Metodología

La metodología aplicada es de tipo descriptivo, producto de la investigación y el análisis a las herramientas de la auditoría forense y su aplicación para identificar y evaluar los riesgos presentes en los ciberataques.

Fase 1. Para llevar a cabo la investigación en la cual se identifican y se evalúan los riesgos presentes en los ciberataques se realizó la búsqueda en diferentes bases de datos de artículos científicos, y en páginas de internet de reconocida trayectoria.

Fase 2. Procesos de investigación en los artículos informativos, circulares de prevención de lavados de activos y ciberataques de la DIJIN de la Policía Nacional de Colombia, para conocer con casos prácticos en la utilización de las herramientas de la auditoría forense.

Fase 3. A través de un estudio de caso y con las investigaciones realizadas detectar los procesos generados, los riegos latentes y las herramientas utilizadas en la auditoría forense.

Normatividad en la prevención y control de los ciberataques

En Colombia se han implementado mecanismos para proteger a los usuarios informáticos de posibles ataques que afecten su integridad, su estabilidad económica y social; frente a una globalización tecnológica donde información tan privada puede ser hurtada y mal manejada por posibles delincuentes informáticos que se encuentran diariamente en el mundo cibernético.

En la tabla 1 se identifican las leyes que en Colombia se han creado y redireccionado para combatir el ciberataque.

La normatividad que regula la información en bases de datos y la manipulación adecuada de la misma es implementada y actualizada año tras año por la evolución inevitable de nuevos ataques a los sistemas informáticos; asimismo, ha llevado al Estado en cabeza del Presidente de la República a la redacción de una serie de decretos, junto con la Comisión Digital (desde el 2014), para definir la estructura de la Agencia Nacional de Seguridad Cibernética Este trabajo está coordinado desde los ministerios de Defensa, Justicia y TIC, buscando modernizar las entidades del Estado y prevenir ataques de hackers o actos de corrupción (TECNÓSFERA, 2014).

Por ende, Colombia se ha integrado a la comunidad internacional a través de los diferentes encuentros que exponen los mecanismos apropiados para combatir los ciberataques, desarrollando participación integral al establecer

Tabla 1. Marco Normativo aplicado a la seguridad informática en Colombia.

Norma	Aplicación	Contenido
Constitución Nacional de la Republica de Colombia de 1991 Artículo 15.	Garantizar el derecho a la intimidad, personal familiar y a su buen nombre	El Estado debe garantizar la actualización y rectificación de información recogida en bases de datos y en archivos de entidades públicas y privadas
Ley 527 de 1999 "Por la cual se reglamenta el acceso y uso de mensajes de datos, comercio electrónico y firmas digitales…"	Comercio electrónico	Se considera que la información consignada en un mensaje de datos integra, si esta ha permanecido completo e inalterada; el grado de confiabilidad requerido, será determinado por a la luz de los fines para los que se generó la información. (Congreso de la República de Colombia, 1999).
Ley 1266 de 2008 "Por la cual se reglamenta el manejo de la información en base de datos…"	Habeas Data	La calidad de los datos suministrados y el acceso a la información, se sujete a los deberes y responsabilidad previstos para garantizar la protección de los derechos del titular de dichos datos. (Congreso de la República de Colombia, 2008).
Ley 1480 de 2011 "Por la cual se expide el Estatuto del consumidor…"	Consumidor, comercio electrónico y publicidad	Regulación de ventas a través del comercio electrónico, determinando las condiciones mínimas para la operación de la información pública de precios de los productos ofrecidos por este medio, del manejo de la información del consumidor evitando que sea manipulado mediante los diferentes ciberataques existentes (Congreso de la República de Colombia, 2011).
Ley 1453 de 2011 "Por la cual se dictan otras disposiciones en materia de seguridad…"	Seguridad Ciudadana	Control de la manipulación de datos a través de las redes de telecomunicaciones y proceder a la recuperación de dicha información desde cualquier medio de almacenamiento físico o digital, para que expertos en informática forense, analicen y custodien los registros con el propósito de obtener elementos materiales probatorios y evidencia física en caso de presentarse delitos informáticos (Congreso de la República de Colombia, 2011).
Resolución CRC 3067 de 2011 "Por la cual se define los indicadores de calidad para los servicios de telecomunicaciones…"	Acceso a internet	Regula el manejo adecuado de los recursos técnicos y logísticos para garantizar la seguridad de la red y la integridad del servicio, para evitar la interceptación, interrupción e interferencia del mismo, por ende deberá informar al usuario final las condiciones adoptadas en relación al servicio prestado tales como el uso de firewalls. Filtros antivirus y la prevención del spam, phishing, malware entre otros (Comisión de Regulación de Comunicaciones, 2011)

Fuente: (Comisión de Regulación de Comunicaciones de la República de Colombia, 2015). Tabla. Recuperado y adaptado.

los instrumentos internacionales como alternativa para desarrollar los modelos de seguridad en fraudes informáticos.

El panorama mundial en materia de seguridad cibernética y delito cibernético en el 2013, evalúa las tendencias más importantes en lo que respecta a las amenazas cibernéticas y a quienes afectan desde instituciones gubernamentales, hasta empresas privadas y usuarios individuales. Asimismo, en la siguiente figura, se observa los informes generados en los encuentros internacionales asumidos por Colombia, para contrarrestar los ciberataques. (Organización de los Estados Americanos, 2014)

Figura 1. Instrumentos Internacionales en orientación para el aseguramiento de la información digital. Fuente: (Comisión de Regulación de Comunicaciones de la República de Colombia, 2015) (figura) Recuperado y modificado por los autores.

Ahora bien, se observa que a nivel mundial los esfuerzos para reforzar la ciberseguridad en los países no cesa, y es así como la OEA presentó el pasado 21 de enero de 2015 en la reunión anual del Foro Económico Mundial realizada en Davos, Suiza, el programa de seguridad cibernética de la OEA para los países de América Latina y el Caribe, dado que es la región del mundo donde Internet se está expandiendo a mayor velocidad y se busca que en la región se elabore una política integral de seguridad cibernética (Organización de los Estados Americanos, 2015).

Herramientas de auditoría forense con ayuda de computadora

Actualmente los ataques cibernéticos han aumentado considerablemente identificando procesos como entidades legalmente constituidas para realizar sus actividades delictivas. Un acto muy común en los ciberataques es el robo

de identidad dejando pérdidas significativas para los usuarios de dichas entidades, ya que el riesgo es directamente relacionado con pérdidas económicas e implica que las víctimas se vean involucradas en procesos ilícitos afectando su reputación legal.

Las Técnicas de Auditoría Asistidas por Computador (TAAC'S), son herramientas usadas por el auditor dentro de los procedimientos generales desarrollados en la auditoría para obtener datos importantes que se encuentran en los sistemas de información de una entidad. Estos datos pueden ser transacciones, archivos de texto u otros archivos; con el propósito de realizar pruebas de controles o procedimientos sustantivos y así conseguir evidencia de la existencia y operación de dichos controles. (Duque, TAACs, 2013).

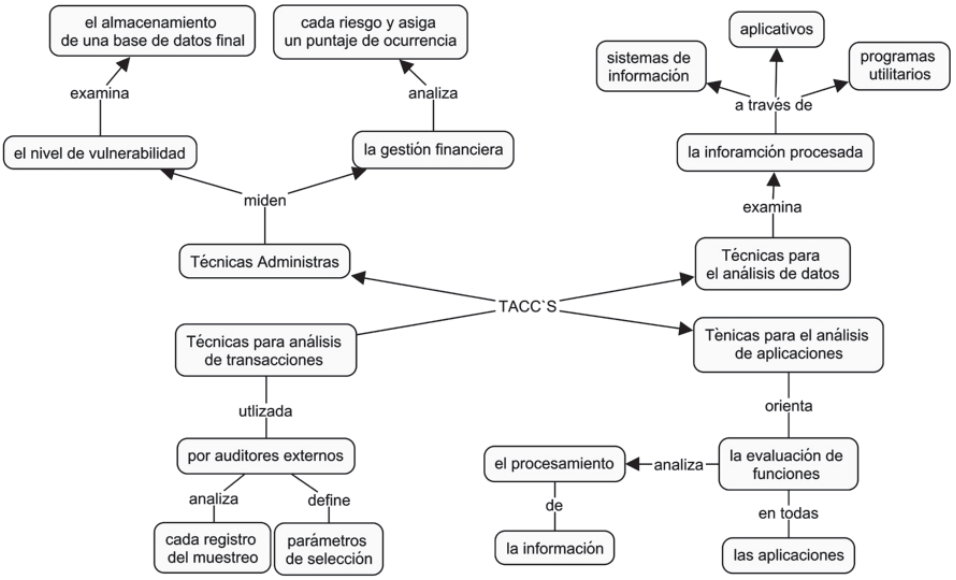

Figura 2. Clasificación de las TAAC'S como herramientas en la auditoría forense. Fuente: (Universidad Nacional, 2013) Figura. Recuperado y modificado por los autores.

En la planeación de la auditoría, el auditor debe considerar una combinación apropiada de técnicas de auditoría manuales y con ayuda de del computador. En la determinación de usar o no las TAAC'S los factores a ser considerados incluyen: conocimiento del computador, pericia y experiencia del auditor, disponibilidad de las TAAC'S y equipo de computación adecuado, imposibilidad de pruebas manuales, efectividad, eficiencia y oportunidad (Quiroz, 1996).

Igualmente, las técnicas CAAT'S se definen como un conjunto de procesos ordenados lógicamente para apoyar las actividades estimadas en el planteamiento de la auditoría forense. El auditor debe incluir en su aplicación: la utilización de software genérico de auditoría, generadores de datos de prueba y técnicas de pruebas integradas.

Para su documentación las CAAT'S siguen una serie de parámetros que ayudan al auditor a organizar la información, estos pueden ser un listado de programas que se deberán utilizar, flujo gramas, informes de muestras, diseños de archivos y registros, definición de campos, instrucciones de operación (Biblioteca Central Cátedra de Ingeniería, 2013).

La figura 3 presenta la información que evidencia el nivel de riesgo en el momento del análisis de los datos del muestreo.

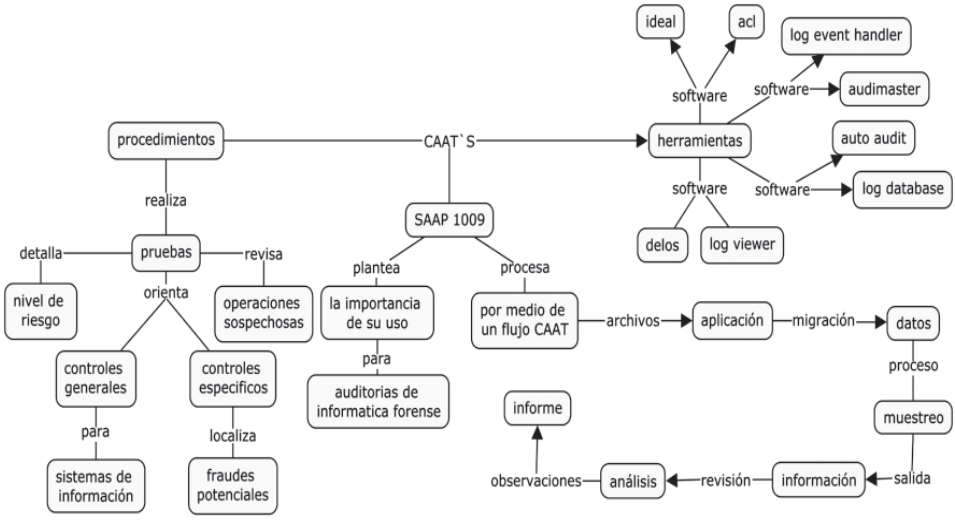

Figura 3. Procedimientos utilizados en las herramientas de auditoría forense. Fuente: (Computer Assisted Audit Techniques CAAT, 2013). Recuperada y adaptada por los autores.

Cuando se realiza una auditoría las CAAT'S incluye distintos tipos de herramientas y de técnicas, las que más se utilizan son los software de auditoría generalizado, software utilitario, los datos de prueba y sistemas expertos de auditoría. Las CAAT´S se pueden utilizar para realizar varios procedimientos de auditoría incluyendo: el control de aplicaciones, seleccionar y monitorear transacciones, verificar datos, analizar programas de las aplicaciones, auditar centros de procesamiento de la información, auditar el desarrollo de aplicaciones que se integran a la seguridad informática (Cabrales, 2013).

Resultados

Los ciberataques hoy en día generan su auge en la sociedad, los hackers utilizan estas modalidades para delinquir e incurrir en hurtos significativos o millonarios hacia las personas o entidades bancarias. Por este motivo las entidades han desarrollado diferentes mecanismos de control y prevención para contrarrestar esta modalidad de fraude; toda entidad debe desarrollar sus políticas, manuales y procedimientos frente al control de las operaciones que se consideren sospechosas.

No obstante las entidades deben tener control sobre todas las actividades que realicen sus empleados, en la documentación y equipos que salen de las oficinas, en los correos electrónicos institucionales y en la red interna y externa. Uno de los factores más relevantes en este tipo de fraude es la seguridad con la que cuenta una empresa no solo en proteger su información a través de canales informáticos sino también de las instalaciones físicas ya que por estos medios se pueden cometer diferentes tipos de ataques que conllevan a acciones destructivas para la entidad.

Los ciberataques como su nombre lo indica son las acciones delictivas que se comenten por los diferentes medios para acceder a información personal y financiera de las personas, pero esta modalidad de fraude no solo se da para entidades financieras, uno de los medios utilizados para generar este tipo de fraude son los sitios web de citas, por lo general las personas que utilizan estos sitios lo realizan a través de un dispositivo móvil como lo es su celular y estos guardan información personal como contraseñas, usuarios etc. que pueden ser utilizados por el hacker para conseguir acceso a la información personal como fotos del dispositivo, micrófonos y almacenamiento de archivos.

En la prevención de este tipo de fraude, la auditoría forense se encarga de presentar las herramientas necesarias que ayuden a establecer el control, prevención y detección de los riesgos que se presentan en los ciberataques, mediante las respectivas políticas de funcionamiento que minimicen el nivel de estos riesgos, considerando que los diferentes malware que afectan a los usuarios es la esencia de la inseguridad para la información financiera, comercial y personal, el cual produce un crecimiento constante del manejo malintencionado de los datos.

Herramientas de auditoría forense para la identificación y evaluación de los riesgos presentes en los ciberataques.

Para obtener información personal o financiera de las personas el ciberdelincuente debe contar con herramientas que generen opciones para que este acceda a todo el historial de su víctima, dentro de estas ayudas se

encuentra el software malicioso- malware-, que por su características informáticas puede estar oculto en los archivos adjuntos en el correo electrónico una vez abierto este archivo adjunto se empiezan a ejecutar una serie de funciones programadas en el sistema operativo de este software y en muchas ocasiones se vuelve casi invisible para el antivirus al realizar copias exactas de procesos en otros programas.

Es de suma importancia tomar precauciones y no abrir correos de dudosa procedencia ya que para ejecutar este tipo de actos los ciberdelincuentes deben generar cadenas de correos con un asunto llamativo hacia la víctima y pueden usar diferentes marcas o empresas reconocidas nacional e internacionalmente para llevar a cabo su invasión a la privacidad.

La función de este software es capturar todos los registros que se realicen por medio del teclado y la navegación virtual realizada por el usuario, una vez analizada toda la información este sistema procede a crear ciertos archivos con una denominación en particular "server.exe" que contiene toda la información y de igual forma tiene como función él envió de la misma suministrada inconscientemente por el usuario o víctima y es almacenada en el servidor, que contiene una configuración especifica que es de utilidad para el ciberdelincuente.

Igualmente este archivo genera aperturas a puertos del equipo y el delincuente tendrá un acceso remoto total. Si el computador se encuentra configurado para realizar ingresos a portales bancarios de los cuales solo se puede acceder mediante un token que proporcionara claves de ingreso generando seguridad este también puede supervisar cada sesión (Dirección de Investigación Criminal e Interpol, 2014).

En el encargo de auditoría forense, para identificar los riesgos presentados en el sistema malware, el auditor debe examinar los ordenadores con las herramientas de administración del sistema; pero este proceso conlleva a una posible modificación de datos y llega a alterar pruebas. Así mismo, de deben adoptar tres pasos para enfocar el análisis forense:

a) Se inicia con una copia exacta de los datos mediante un soporte digital, sin realizarle modificaciones en el origen de los datos. b)A través de software especial para la auditoría forense, se efectúa el procedimiento para el levantamiento de las pruebas, como puede ser la recopilación de contraseñas y archivos borrados y así, obtener información inicial desde el sistema operativo y por último se elabora un informe por escrito con las evidencias halladas en el análisis y se presenta las conclusiones sustraídas de los resultados arrojados por el software, sin dejar de suministrar la restauración de los hechos o incidentes que se encontraron en la información.

Es importante que el software elegido para la investigación sea garante de una evidencia confiable, suficiente y competente, en el encargo de la auditoría

forense con herramientas que satisfagan los requisitos para detectar los posibles fraudes.

Por consiguiente a través de la matriz de riesgo (tabla 2) se ejemplifica los peligros que se pueden presentar en diferentes situaciones en las cuales se ve expuesta una entidad hoy en día como lo es la inseguridad que se presenta en la sociedad con el delito de lavado de activos y financiación del terrorismo. Lo anterior genera una gran preocupación para el sector bancario porque son utilizados para estos actos delictivos, por este motivo se deben identificar los riesgos y controles para la mitigación de situaciones.

Tabla 2. Matriz de identificación de riesgos**.**

Descripción del Riesgo	Causas	Efectos del Riesgo (Consecuencias)	Control Implementado (Medidas Preventivas y Correctivas)	Clasificación
Tecnológico	Conocimiento de contraseñas	Accesos no autorizados a correos electrónicos, portales bancarios, plataformas internas.	Contar con los controles necesarios para detectar virus generados por los Malware, brindar información a los colaboradores de la entidad la precaución de no abrir correos de dudosa procedencia.	Riesgo alto
Físicos	Robo de documentos	Filtrar información relevante para las compañías, ingreso a las instalaciones de la entidad sin autorización, obtención de documentos que revelen operaciones de los clientes.	No permitir el ingreso de personal no autorizado a las instalaciones físicas de la entidad,	Riesgo alto

Sigue...

Viene...

Descripción del Riesgo	Causas	Efectos del Riesgo (Consecuencias)	Control Implementado (Medidas Preventivas y Correctivas)	Clasificación
Fallas humanas	No identificación de riesgos	No contar con los controles adecuados para salvaguardar los riesgos, establecer y dar cumplimiento a las políticas establecidas por la entidad.	Cumplir con los procedimientos establecidos por la entidad como los horarios de arqueos de caja, horarios de aperturas de oficinas después de haber culminado la atención del servicio al cliente, realizar auditorias recurrentes para la identificación de procesos que no se estén llevando a cabo, segregación de funciones en diferentes empleados	Riesgo alto

Fuente: (Los autores, 2015).

Con el fin de detectar los riesgos una entidad, se debe generar este proceso por consiguiente se evalúan los escenarios en los cuales se puede ver inmersa la entidad las causas y consecuencias para minimizar estas eventualidades. Con la información generada a través de esta herramienta la entidad puede verificar si cuenta con los procedimientos adecuados para contrarrestar esta situación, si por el contrario no cuenta con estos, debe formular medidas de control preventivas.

Herramientas de auditoría forense que ayuden a detectar los riesgos en los ciberataques

Las herramientas de auditoría forense promueven el aseguramiento en cualquier medio digital, hallando evidencias sin alterar la información original. Los

datos deben ser catalogados para proceder a su análisis y de la mano, realizar la documentación de las pruebas que se realicen y que apoyen las hipótesis, justificando el análisis que se presentará al finalizar el documento.

Al iniciar el procedimiento se debe tener en cuenta la protección de los derechos a terceros para que estos no sean vulnerados, en el caso en que se pueda constituir un elemento de prueba fundamental, ante tribunales judiciales. Las herramientas de software en la práctica de auditoría forense varían en la búsqueda, recuperación y clasificación de datos fundamentales.

La recuperación de información se debe basar en el aseguramiento de la información y control interno mínimo; a partir de lo anterior, la auditoría forense será confiable, garantizando la información necesaria para investigar operaciones sospechosas y materializar su riesgo.

Estas herramientas ofrecen la obtención de datos informáticos; en esencia se procura mantener una infraestructura y su aplicación siguiendo los parámetros determinados por las Normas Internacionales de auditoría –NIAS-. De acuerdo a la NIA Sección 1003, se determinan mecanismos para el control y administración en base de datos así:

Recuperación de copias de seguridad; detección de procesos que no cumplan con el anti-desastre de información virtual; elaboración de filtros de corriente determinando una clasificación para la mayor vulnerabilidad de los procesos para protección y control de la información.

De igual forma, la comprobación del nivel de seguridad de sistemas de protección en conexiones a internet como lo son el firewall y antivirus, así divisar el nivel de acceso de hackers y software malintencionado; revisión de filtros en correos electrónicos para información considerada SPAM o de procedencia desconocida no apta para corporaciones y análisis para detectar fallos en la seguridad de las redes de comunicación por medio de aplicaciones creadas para este objetivo.

Por consiguiente, estas herramientas y el análisis que brindan posterior a la recepción de la información, permiten identificar los delitos informáticos más relevantes y el riesgo inherente que presentan; en la figura 4 se observa que se definen las categorías de dichos delitos y cómo proceden para afectar a la sociedad.

Los delitos informáticos también se encuentran clasificados según su categoría de riesgos presentes en la comunidad; ahora bien, las herramientas de auditoría permiten detectar diferentes delitos informáticos tales como: claves programáticas que actúan como espías que se pueden encontrar en diferentes virus como troyanos, incluyendo el software espía; estafas a través de subastas en línea por medio de la receptación de elementos hurtados como venta de productos de dudosa procedencia a través de la red en internet.

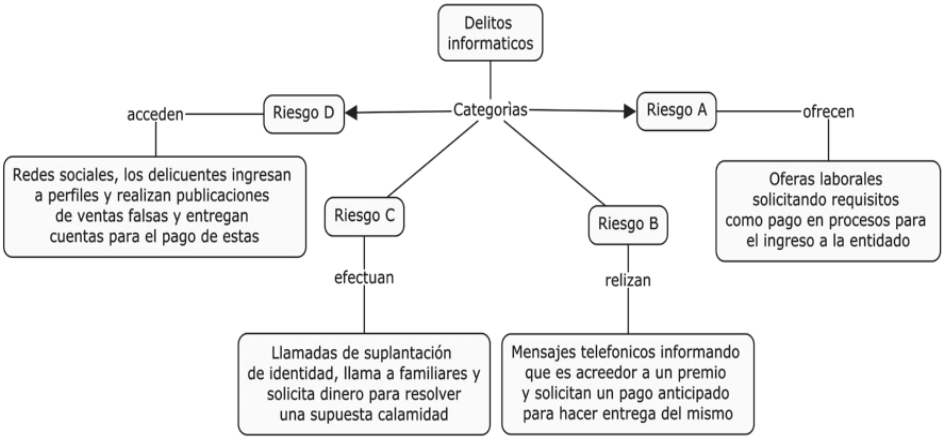

Figura 4. Riesgos informáticos presentes en Colombia y su proceso para ataques cibernético. Fuente: (Policía Nacional Dirección de Investigación Criminal e Interpol, 2014) Figura. Recuperado y modificado por los autores.

Por consiguiente, la divulgación indebida de contenidos se ve reflejado en los sitios como café internet, quienes prestan estos servicios desde equipos que no cuentan con los diferentes controles para la privacidad de la información; asimismo, la pornografía infantil en internet, se presenta a través de comunidades vinculadas a diferentes chats o foros.

Considerando también la violación a los derechos de autor que en este caso el delincuente realiza diferentes copias de juegos, películas, canciones etc.; por esa razón se vender programas protegidos por las leyes de la propiedad intelectual, así se evita dicha piratería (Comisión de Regulación de Comunicaciones de la República de Colombia, 2015).

Antiguamente la comprobación de la gestión, control y actividad económica-financiera de las empresas se realizaba mediante largos, costosos y exhaustivos procesos de auditoría financiera; con la implantación de sistemas informáticos se detectan entradas y salidas generadas determinando si son objeto o no de manipulación. Una auditoría forense para la seguridad informática evalúa dichos sistemas identificando errores y fallas analizando su nivel de riesgo (Bernal Gutierrez & Arandia Forero, 2006).

A continuación, se presenta una clasificación detallada de las herramientas de auditoría forense para evaluar fraudes, corrupciones, ciberataques e innumerables formas que existen para cometer delitos y fraudes. En tal sentido, se determinan herramientas orientadas y relacionadas con los campos de acción informáticos en los que puede presentar servicio el auditor forense.

Tabla 3. Procesos de la auditoría forense en la detección de ciberataques.

Tipo de proceso	Procedimiento
Análisis de seguridad en la red	Se contrasta el nivel de seguridad y privacidad de las redes locales y corporativas de carácter interno
Análisis de la eficiencia de los sistemas y programas informáticos	Se comprueba el nivel de resistencia mediante el acceso a los sistemas y se verifica la intrusión no deseada.
Análisis de riesgos	Se detectan amenazas y elementos de seguridad de entrada y salida de datos
Análisis ante perdidas, fraude y ciberataques	Se reconstruye el proceso de penetración en el sistema, valorando los daños ocasionados para creas medidas de seguridad, directivas, preventivas y correctivas.
Análisis de la seguridad física	Se analiza el grado de seguridad que ofrece las entradas exteriores; equipos, servidores, programas, sistemas operativos
Análisis de la seguridad de datos y programas	Se comprueba la vulnerabilidad del acceso a la web
Elaborar Políticas de seguridad	Se determine los alcances efectuados en la identificación de elementos inusuales mediante los mecanismos de control más acertados para el desarrollo de una seguridad de alto nivel.
Elaborar Protocolo de riesgos	Se efectúa un seguimiento adecuado de las transacciones, relacionando frecuencia, volumen y características de las mismas; determinando la procedencia de las operaciones sospechosas

Fuente: (Bahamontes, 2013). Tabla. Recuperado y adaptado por los autores.

Los auditores forenses, en su encargo usan gran cantidad de técnicas para descubrir evidencias, incluyendo herramientas de software que automatizan y aceleran el análisis cibernético como el rastreo de información en la memoria y archivos digitales, análisis de datos "borrados" en el disco duro de los computadores.

Los riesgos presentes en los ciberataques, mediante herramientas de auditoría forense, a partir de un caso estudio

El CTI de la Fiscalía de Cali desarticuló una organización delincuencial especializada en robos a entidades bancarias, responsable de hurtar al menos $10 mil millones de cuentas empresariales. La investigación, indicó Rodríguez, se inició en el 5 de octubre de 2013, luego de que el Banco de

Bogotá denunciara ante la Fiscalía el intento de hurto de $1600 millones por parte de un empleado de la entidad que había realizado una serie de consignaciones ilegales a varias cuentas. Luego de la denuncia, la Unidad de Delitos Informáticos del CTI inició un seguimiento al funcionario del banco y, gracias a interceptaciones de llamadas y labores de vigilancia, se pudo determinar que hacía parte de una red que falsificaba cheques, cédulas y que además tenía a varios hackers que se dedicaban a "romper claves" para hurtar electrónicamente cuentas bancarias.

Según investigaciones del CTI, los delincuentes tenían a su disposición una serie de personal quienes eran los encargados de realizar todo el proceso de hurto, debido a que contaban con especialistas en falsificación de documentos y en especial en los cheques bancarios. Los delincuentes llevaban los cheques falsificados al banco y cuando la entidad hacia la verificación del titular de la cuenta, interceptaban las llamadas gracias a un técnico de ETB que abría las cabinas de mantenimiento telefónico y se hacían pasar por el titular de la cuenta.

Asimismo, cuando el teléfono que el banco tenía del titular de la cuenta era un móvil, las autoridades lograron determinar que la banda previamente ya había adquirido los números telefónicos del titular, había interpuesto una demanda por robo con una cédula falsa, y de ese modo accedían a una nueva simcard con el número del verdadero titular de la cuenta. Una entidad bancaria debe seguir pasos para evitar que esto suceda en sus instalaciones aunque los delincuentes eran dirigidos por un empleado que trabajaba directamente en la entidad, los procedimientos deben quedar documentados para evitar estos actos deshonestos.

Para esto se deben implementar medidas de seguridad en este caso fueron vulneradas, ver que se presentan diferentes riesgos: riesgo reputacional el cual se ve afectado el buen nombre de la entidad y riesgo legal, porque puede incurrir en indemnizaciones por los daños ocasionados por el incumplimiento de las normas (Redacción de El País, 2015).

En el caso de las entidades financieras para la prevención de cada proceso delictivo como el lavado de activos y los ciberataques, deben constituir el respectivo manual que se conoce como SARLAFT en cual se relaciona todo el proceso que va a realizar la entidad al momento de generarse situaciones que se consideren sospechosas, por medio de este se minimizan los riesgos y su objetivo es prevenir la entrada al sistema financiero los dineros provenientes de actividades ilícitas para la financiación del terrorismo.

Actualmente estos ataques presentan una gran amenazada en la sociedad, debido a que las entidades financieras son utilizadas como medio para realizar estos atentados. El SARLAFT se compone esencialmente de dos fases: la primera

corresponde a la prevención del riesgo. La segunda corresponde al control cuyo propósito consiste en detectar las operaciones que se pretendan realizar o se hayan realizado para intentar dar apariencia de legalidad. (Superintendencia Financiera de Colombia, 2013).

Para minimizar el riesgo las entidades deben generar políticas para la prevención de ciberataques, actualmente existen listas restrictivas en las cuales se debe consultar para tener un mayor conocimiento del cliente. Las listas restrictivas generan una advertencia para las entidades que deben abstenerse o prestar un cuidado especial a las personas que se encuentren vinculadas a esta lista, en ella se encuentran los individuos que han cometido estos delitos.

La lista ONU: actualmente es la única lista vinculada en Colombia en las cuales se encuentran los individuos vinculados con Alqaeda, Osama Bin ladem y es vigente para Colombia por pertenecer a los postulados de la ONU. Las entidades deben reconocer las transacciones que se consideren sospechosas como los clientes que las realizan para ser reportadas, estas son operaciones que no guardan relación con su actividad.

Estas transacciones se pueden detectar por los comportamientos de las personas porque no se presentan como normales, la persona que esté realizando estas acciones puede también realizar acciones delictivas con la entidad. Por este motivo la entidad debe contar con un sistema de capacitación hacia sus colaboradores, debido a que son la imagen de la entidad y los delincuentes pueden buscar diferentes alternativas para no solo realizar procesos de ataques cibernéticos, sino también generar un riesgo reputacional para la entidad.

Estos procedimientos deben estar debidamente calificados y generados por la entidad pues son la ayuda para no minimizar riesgo para la empresa o sus clientes. Para tener un manejo adecuado de estas operaciones se debe tener en cuenta que la entidad debe tener un conocimiento apropiado del cliente, conocer su actividad laboral para así generar conclusiones si una transacción se puede considerar como sospechosa, el conocimiento del mercado es otro factor que se debe tener en cuenta al momento de analizar los riesgos.

Sin embargo en este caso los clientes eran personas que no estaban reportados en estas listas, por este motivo el procedimiento para detectar anomalías se debía presentar en las oficinas de la entidad puesto que las operaciones internas no deben estar a cargo de un solo empleado, debe haber una segunda instancia quien es la encargada de verificar la veracidad de la información. Los delincuentes buscan el lado más vulnerable para realizar sus actos por este motivo las entidades financieras debe prepararse para posibles dificultades que se presenten, generar pruebas en diferentes escenarios y tener todos los controles establecidos en la entidad.

Conclusiones

El auditor forense debe asegurar que la infraestructura de hardware y conexiones red para la estabilidad en la información compartida y las aplicaciones que interactúan con la seguridad de los datos; integrando a estos en una base de datos que interactúa con varias aplicaciones para evitar su duplicidad y confirmar que estos sean almacenados exitosamente.

Sin embargo, el riesgo reputacional en las empresas se ve perjudicado por diferentes factores entre ellos la seguridad de la información de los clientes de manera que el delincuente puede ingresar a las instalaciones y recolectar la documentación necesaria para estos actos ilícitos; por otra parte la entidad debe contar con un sistema de seguridad que no permita que los hackers ingresen a sus sistemas operativos y capten información de sus clientes.

No solo este tipo de ciberataques se pueden presentar en las empresas también se generan casos para personas, hoy en día el teléfono móvil es muy necesario para realizar actividades diarias, en este incluimos contraseñas, información de las redes sociales que pueden ser utilizadas para cometer actos delictivos. Cada vez son más las personas en el mundo que utilizan el servicio de internet y a la vez aplicaciones para los computadores y los teléfonos móviles por esto aumenta la vulnerabilidad para las personas y las oportunidades para los hackers para conseguir información personal.

En el proceso de evidencias para detectar dichos riesgos es necesario que las entidades prestadoras de servicios en servicios informáticos cuentan con las herramientas de auditoría forense para controlar las seguridad de acceso de los usuarios a la información, detectando las anomalías físicas tales como conexiones internas y externas de telecomunicaciones e infraestructura de equipos; anomalías tecnologías en el procedimiento para el mantenimiento de sistemas de datos, minimizando el nivel de vulnerabilidad presente en los ciberataques.

La investigación de un fraude financiero será obligatoria dependiendo del 1) el tipo de fraude; 2) el entorno en el que fue cometido (público o privado); y, 3) la legislación aplicable. Un trabajo de auditoría forense también puede iniciar directamente sin necesidad de una auditoría previa de otra clase, por ejemplo en el caso de existir denuncias específicas.

Bibliografía

Ayala, J. B. (8 de mayo de 2008). *na.teiia.org.* Recuperado el 18 de octubre de 2015, de na.teiia.org: https://na.theiia.org/translations/PublicDocuments/Auditoria_Forense_Una_Misi%C3%B3n_JBadillo_Mayo08(14023).pdf

Bahamontes, Á. (15 de agosto de 2013). *Asociación Nacional de Tasadores y Peritos Judiciales Informáticos*. Recuperado el 17 de noviembre de 2015, de http://www.antpji.com/antpji2013/index.php/articulos2/111-auditoria-de-seguridad-informatica

Bernal Gutiérrez, S. C., & Arandia Forero, N. M. (2006). La auditoría forense como herramienta en la detección del lavado de activos en el sector bancario. Bogotá D.C., Cundinamarca, Colombia.

Biblioteca Central Cátedra de Ingeniería. (2013). *ub.edu.ar*. Obtenido de http://www.ub.edu.ar/catedras/ingenieria/auditoria/softaudit/softaudit.htm

Caat, C. A. (2015). *olea.org*. Recuperado el 18 de octubre de 2015, de olea.org: http://olea.org/~yuri/propuesta-implantacion-auditoria-informatica-organo-legislativo/ch03s04.html

Cabrales, C. A. (2013). *Aditoría informatica: Conceptualización*. Valle del Cauca, Buenaventura.

Comisión de Regulación de Comunicaciones. (18 de mayo de 2011). Resolución 3067 DE 2011. *Diario Oficial* (48073).

Computer Assisted Audit Techniques CAAT. (2013). Recuperado el 25 de 10 de 2015, de http://olea.org/~yuri/propuesta-implantacion-auditoria-informatica-organo-legislativo/ch03s04.html

Comisión de Regulación de Comunicaciones de la República de Colombia. (2015). *Identificación de las posibles acciones regulatorias a implementar en materia de Ciberseguridad.*

Congreso de la República de Colombia. (211 de agosto de 1999). Ley 527 de 1999. *Diario Oficial* (43.673).

_____. (31 de diciembre de 2008). Ley estatutaria 1266 de 2008. *Diario Oficial* (47.219).

_____. (12 de octubre de 2011). *Secretaria del Senado*. Obtenido de http://www.secretariasenado.gov.co/senado/basedoc/ley_1480_2011.html

_____. (24 de junio de 2011). *Secretaría del Senado*. Obtenido de http://www.secretariasenado.gov.co/senado/basedoc/ley_1453_2011.html

Dirección de Investigación Criminal e Interpol. (2014). *Boletín Informativo Cibercrimen - Malware: Cambio de Paradigma*. Boletín, Policía Nacional de Colombia, Bogotá D.C.

Dueñas, S. M. (2009). Mecanismos de contabilidad para prevenir y detectar el lavado de activos en Colombia. Bogotá D.C., Colombia.

Duque, N. (2013). *virtual.unal.edu.co*. (U. N. MANIZALEZ, Productor) Recuperado el 18 de octubre de 2015, de virtual.unal.edu.co: http://www.virtual.unal.edu.co/cursos/sedes/manizales/4060035b/und_5/html/taacs.html

_____. (s.f.). *virtual.unal.edu.co*. (U. N. MANIZALEZ, Productor) Recuperado el 18 de octubre de 2015, de virtual.unal.edu.co: http://www.virtual.unal.edu.co/cursos/sedes/manizales/4060035b/und_5/html/taacs.html

International Standard on Auditign. (2002). Recuperado el 18 de octubre de 2015, de http://www.ccpsucre.org.ve/LeyesReglamentos/leyes/NormativaInternacional/5NIC-NIIFInterpretaciones/NIATraduccion/sec1009tecnicasauditoriaayuda computadora. pdf

International Standard on Auditing. (2002).

Maldonado, M. (2003). Auditoría Forense: Prevención e Investigación de la Corrupción Financiera. En M. Maldonado, *Auditoría Forense: Prevención e Investigación de la Corrupción Financiera* (pág. 9). Quito, Ecuador: Editorial Luz de América.

Ministerio de Comercio Exterior, Industria y Turismo. (4 de diciembre de 2012). *sic.gov.co*. Recuperado el 9 de 11 de 2015, de http://www.sic.gov.co/drupal/sites/default/files/normatividad/Resolucion_76434_2012.pdf

Organización de los Estados Americanos. (junio de 2014). *symantec*. Recuperado el 11 de noviembre de 2015, de https://www.symantec.com/content/es/mx/enterprise/other_resources/b-cyber-security-trends-report-lamc.pdf

_____ (21 de enero de 2015). *oas.org*. Recuperado el 11 de noviembre de 2015, de http://www.oas.org/es/centro_noticias/comunicado_prensa.asp?sCodigo=C-012/15

Policía Nacional Dirección de Investigación Criminal e Interpol. (2014). *Anatomía de las estafas cibernéticas*.

Quiroz, L. G. (1996). Informática y auditoría para las ciencias empresariales. En L. G. Quiroz, *Informática y auditoría para las ciencias empresariales*. UNAB.

Redacción de El País. (22 de mayo de 2015). Cayó red que robó mas de $10 mil millones a bancos. *EL PAÍS*.

Superintendencia Financiera de Colombia. (2013). Capítulo 11: Instrucciones relativas a la administración del riesgo de lavado de activos y financiación del terrorismo. *Circular Externa 010 de 2013*.

Tecnósfera. (11 de julio de 2014). Colombia se prepara para enfrentar los ciberataques. *EL TIEMPO*.

Universidad Nacional. (2013). *Virtual.unal.edu.co*. Recuperado el 20 de octubre de 2015, de http://www.virtual.unal.edu.co/cursos/sedes/manizales/4060035b/und_5/html/taacs.ht