Revista Sinergia 2018, Edición 4, p. 108-129. ISSN: 2665-1521

# PRESENTE Y FUTURO DE LA EVIDENCIA INFORMÁTICA: ANÁLISIS FRENTE A LAS COMPETENCIAS DEL AUDITOR

**Fernando Gutiérrez Pórtela**
Estudiante Doctorado de Ingeniería de la Universidad Autónoma de Bucaramanga. Profesor de la Universidad Cooperativa de Colombia del programa de Ingeniería Civil. Integrante del Grupo de investigación AQUA.
Fernando.gutierrez@campusucc.edu.co

**Jennifer Alexandra Alvarez Porras**
Estudiante de décimo semestre pregrado. Programa contaduría pública
Universidad cooperativa de Colombia- sede Ibagué - Espinal
jennifer.alvarezp@campusucc.edu.co

**Uriel Mauricio Lopez Gúzman**
Estudiante de décimo semestre pregrado. Programa contaduría pública.
Universidad cooperativa de Colombia- sede Ibagué - Espinal.
mauricio.lopez@campusucc.edu.co

# PRESENTE Y FUTURO DE LA EVIDENCIA INFORMÁTICA: ANÁLISIS FRENTE A LAS COMPETENCIAS DEL AUDITOR

## Resumen

El objetivo de este artículo es analizar el presente y futuro de la evidencia informática y el análisis frente a las competencias del auditor. Metodológicamente este artículo es descriptivo y documental ya que redacta la importancia en la actualización del manejo y control de los sistemas informáticos, como incremento de conocimientos informáticos, con el fin de realizar una buena auditoria informática soportada en evidencia suficiente y probatoria. Para el desarrollo de este artículo se valorara los riegos del auditor frente a la evidencia informática, como la evaluación de los posibles riesgos que se puedan presentar en la compilación de la evidencia informática; se describirá el procedimiento para la obtención, análisis y presentación de la evidencia informática, como medio de apoyo para la planeación y ejecución de una auditoria informática. Por último se valorara la evidencia informática del perito contable en el proceso judicial, determinando la calidad y el tipo de evidencia informática compilada y presentada ante el juez para soportar la acusación de los delitos informáticos.

**Palabras clave:** Evidencia informática, auditoria, tecnología

# PRESENT AND FUTURE OF COMPUTER EVIDENCE: ANALYSIS AGAINST THE AUDITOR'S COMPETENCES

## Abstract

*The main objective of this article is to analyze the present and the future of digital evidence and the analysis in front of the auditor's competences. Methodologically speaking, this is a descriptive article, and at the same time a documentary, since it compiles the importance of updating the management and control of computer systems, as increasing computer knowledge, in order to conduct a proper computer auditing supported by enough evidence. In contemplation of the development of this article, the risks the auditor is to face, in front of the digital evidence, are to be taken into account as well as the possible risks that may be presented while compelling the digital evidence. The procedure to gather analysis, and presentation of digital evidence will be furthermore described. Last but not least, the digital evidence of the chartered accountant on legal proceedings, determining quality and the kind of digital evidence gathered and presented to the court in order to support the accusation of computer-related crimes will be evaluated.*

***Keywords:*** *Evidence, computers, audit, technology*

## INTRODUCCIÓN

La evidencia informática desde algunas décadas ha revelado grandes conocimientos frente a la utilización y el desarrollo del software y toda la parte sistematizada que se maneja en una entidad proveniente de una auditoria donde abarca la comprobación sobre la fiabilidad de la herramienta informática y la utilización que se hace de la misma, simultáneamente esto deduce una programación y planificación para la confrontación de los procesos y procedimientos que se efectúan bajo la informática permitiendo que sea más ágil el manejo contable, operacional y financiero. Piattini, (S.f.), refiere lo siguiente "Una de las tendencias actuales más significativas es la que se dirige desde una sociedad industrial hacia la llamada sociedad de la información." donde se vincula toda la tecnología y su gran efecto en las disposiciones de la globalización en las que el mundo se encuentra hoy, donde su objetivo primordial es la manipulación de la información.

Para ello el contador público en su experticia de auditor deberá preparar sus papeles de trabajo que conforten la evidencia informática mediante una gran cuantía de cualidades donde las características humanas se encuentran basadas en conocimientos de las técnicas de auditoria y otra muy importante como las competencias en materia informática donde unidas las dos desencadenan un fuerte enlace de actividades y procedimientos elocuentes en vista de lo que comprende la informática y su manipulación en la entidad para llegar obtener el resultado requerido.

En el ámbito judicial la evidencia informática es analizada como parte esencial en las programaciones que son derivados de los procedimientos electrónicos esenciales en una entidad con el fin de ser más competitivos con la información para ello el auditor tiene un papel, posición y responsabilidad compleja frente a lo legal por ello se refiere a las ISACF[1] como fuente de apoyo frente al trabajo de auditoria a desarrollar y para ello las ICAC[2] de la mano de la Agencia de protección de datos y el código de procedimientos civil con la ley de delitos informáticos.

Considerando lo anterior el estudio explica el análisis del presente y futuro de la evidencia informática, donde la sociedad actual conserva el dominio de la tecnología como motor de cambio acelerado donde la recolección de la información a través de

1. *Information Systems Audit and control Foundation*
2. *Normas técnicas de Auditoria*

la tecnología como pilar principal es el fruto de la unión de la información mediante un proceso de planeación, ejecución y un informe como base de la función de la auditoria informática soportado con papales de trabajo o documentación y así encarar el informe y dar su opinión referente al caso.

## LA EVIDENCIA INFORMÁTICA A TRAVÉS DEL TIEMPO

En términos simples, la evidencia hace énfasis al resultado de los procedimientos y técnicas utilizadas en la auditoria, mediante las distintas pruebas sustantivas y de cumplimiento manejadas por el contador público, como base para la opinión en una auditoria informática documentada por diferentes fuentes para una conclusión de acuerdo a su juicio profesional.

Blanco (2005), expresa que “El verdadero impulso a la auditoría moderna lo dio el Renacimiento, con el auge del comercio, el desarrollo de la Contabilidad, prima hermana de la Auditoría, y el auge del capital financiero y de préstamo” (p. 22). Es necesario recalcar que desde tiempos remotos la revisión detallada de los registros en las distintas operaciones que determinan el manejo de una entidad en sus diferentes actividades nace de la necesidad de controlar y revisar los activos, por ello nació el nombre de auditor de quien se dedujo que escuchaba los informes. Hay que mencionar, además que entre los años 3000 a 2008 a.C. se descubrieron documentos que notificaban los registros de inventarios y libros de cuentas basados de escrituras cuneiformes en tablas de Arcilla.

Dentro de la evolución de la auditoria y su trayectoria tan rigurosa en la información contable, en la veracidad de las estadísticas y en un análisis más profundo de la economía se formaliza la auditoria de sistemas que está basada en la tabulación y computarización de esta, permitiendo que sea más organizada y detallada de la información.

En la auditoria de sistemas informáticos se instruyen los contadores públicos en un reto mayor, dando paso a nuevos ideales, a conocimientos implícitos sobre la informática y tratamiento de la información ya computarizada es por ello que, los auditores se adaptaron a esa nueva tecnología y desarrollaron técnicas y métodos adecuados a ellas, para asegurar la veracidad, integridad y completitud de las

informaciones procesadas (Blanco, 2005). Frente a la implementación de la información sistematizada y su impacto Moreno (2009), argumenta que "En 1890 Herman Hollerith desarrolla una máquina electromecánica de tabulación para procesar la información del censo de 1890 de los Estados Unidos" de donde se infiere que desde esa partida se relacionó los sistemas de tabulación electromecánica por lo que se llevó a cabo distintas actividades para procesar tareas contables.

Años más tarde en 1944 es conocido el primer computador y como resultado exitoso años después se registra un conjunto de prácticas en la auditoria de sistemas que permiten al auditor especificar sus actividades y de tal manera que estudien y se formen, es desde ese momento que el auditor comienza a apropiar sus conocimientos en esa tendencia de tecnología abarcada en la veracidad del aseguramiento de la información, integridad y complejidad de la misma y desarrollarse en su entorno como personal capacitado en la obtención de la evidencia informática proyectado en los distintos papeles de trabajo que dispondrá para tal efecto (Lázaro, 2005)

De esta manera, se puede analizar que mediante la consolidación de la información contable en el ámbito computarizado surge un impactante efecto deducido en la evidencia informática, todo esto confirmado con aquellas actividades que van dirigidas a los procesos, procedimientos y técnicas referidas en la auditoria de una entidad.

Competencias del auditor para la evidencia informática

El auditor como profesional catalogado tiene que basar todos sus principios en habilidades y destrezas en el desarrollo de sus funciones para poner en práctica los conocimientos de temas esenciales que permitan viabilizar un gran trabajo en la auditoria, ya que es el que tiene toda la responsabilidad frente al manejo de la información computarizada.

Parte esencial para el desarrollo de las competencias de un auditor se encuentran desarrolladas en técnicas informáticas basadas en el conocimiento adquirido frente al desarrollo y planeación de una auditoria y por otra parte frente al conocimiento en materia informática.

Derrien (2009), expresa que "requieren de los auditores una amplia competencia técnica en el campo de la informática; métodos de desarrollo, métodos de explotación, características de los principales equipos y software básicos" (p. 220) teniendo en cuenta que el auditor de hoy es un contador con amplia capacidad de innovar e

inculcar proyecciones al buen manejo de la contabilidad en el método computarizado y a su vez lograr mejores resultados en la auditorias que se realicen por lo que su dedicación estará basada en la implementación de conocimientos claves.

En el código de ética profesional en su artículo 35 manifiesta el perfil explícito sobre el contador que en definitiva es el mismo auditor encargado de realizar las actividades contundentes en el proceso de auditoría y con ello los principios esenciales acompañados de varios ítems que hacen que se considere indispensable para tal proceso informático. Marcombo, (2009) expresa lo siguiente “Para el auditor, el paso durante algunos años por las funciones de auditoría informática constituye un «plus» innegable, y será considerada en el futuro como una condición sine qua non ” por lo que limita la autenticidad que este tiene en la parte informática y verifica los constantes cambios positivos y muy rigurosos frente al trabajo que desarrolla, por lo tanto encontramos el siguiente cuadro con temas específicos que detallara al auditor informático.

***Tabla 1. Competencias del auditor en la evidencia informática***

| | | |
|---|---|---|
| Técnica conocimiento informático | Informática básica | Sistemas operativos de las máquinas utilizadas en la entidad que debe auditar |
| | | Conocimientos gen erales sobre hardware de las máquinas existentes en la entidad |
| | | Programas utilitarios del sistema operativo. |
| | Seguridad y protec ción de la información en ambientes informatizados | Seguridad y protec ción física, organizativo-administrativa, por software, por instala ción de equipos y dispositivos, p or construcción y remodelación de locales, mediante medidas educativas y culturales, legales, en tre otros |
| | | Actuación con tra virus informáticos y o tros ataques. |
| | | Elaboración de planes de seguridad y protección y de contingencias ante catá strofes. |
| | Programación de computadoras | Técnicas de programación básicas ( paradigmas básicos: estructurados y orientación a objetos). |
| | | Lenguajes más conocidos y utilizados e n la entidad. |
| | Bases de datos | Modelos fundamentales en la actualidad: relacional, orientados a objetos e hipertextos. |
| | | Características de los gestores de bases de datos empleados en la entidad. |
| | | Protección y seguridad de la información en las bases de datos. |
| | Tecnología de diseño y elaboración de sistemas | Diseño de entradas y salidas de información |
| | | Diseño de procesos automatizados |
| | | Diseño de procedimientos manuales |

| | | |
|---|---|---|
| Técnica conocimiento en la auditoria | Técnicas de auditoria asistida por la computadora | software general y especificos |
| | | Objetivos y amplitud del programa de auditoria |
| | | Métodos de procedimientos existentes y sus caracteristicas |
| | Conocimiento Electrónico | Organizaciones normativas |
| | | Modalidades |
| | | Problemas de seguridad y proteccion de la documentación |
| | Atributos Personales | Ético, es decir, imparcial, honesto, sincero y discreto |
| | | De mentalidad abierta, es decir, dispuesto a considerar ideas o puntos de vista alternativos. |
| | | Diplomático, es decir, con tacto en las relaciones con las personas. |
| | | Perceptivo, es decir, instintivamente consciente y capaz de entender las situaciones. |
| | | Tenaz, es decir, persistente, orientado hacia el logro de los objetivos. |
| | | Seguro de sí mismo, es decir, actúa y funciona de forma independiente a la vez que se relaciona eficazmente con otros. |
| | Procedimientos y técnicas de auditoria | Planificar la auditoría y hacer uso eficaz de los recursos durante la auditoría. |
| | | Representar al equipo auditor en las comunicaciones con el cliente de la auditoría y el auditado. |
| | | Establecer prioridades y centrarse en los asuntos de importancia. |
| | | Verificar la exactitud de la información recopilada. |
| | | Confirmar que la evidencia de la auditoría es suficiente y apropiada para apoyar los hallazgos y conclusiones de la auditoría. |
| | | Evaluar aquellos factores que puedan afectar a la fiabilidad de los hallazgos y conclusiones de la auditoría |
| | | Utilizar los documentos de trabajo para registrar las actividades de la auditoría |
| | | Mantener la confidencialidad y la seguridad de la información. |
| | | Comunicarse eficazmente, ya sea con las actividades lingüísticas personales o con el apoyo de un intérprete |

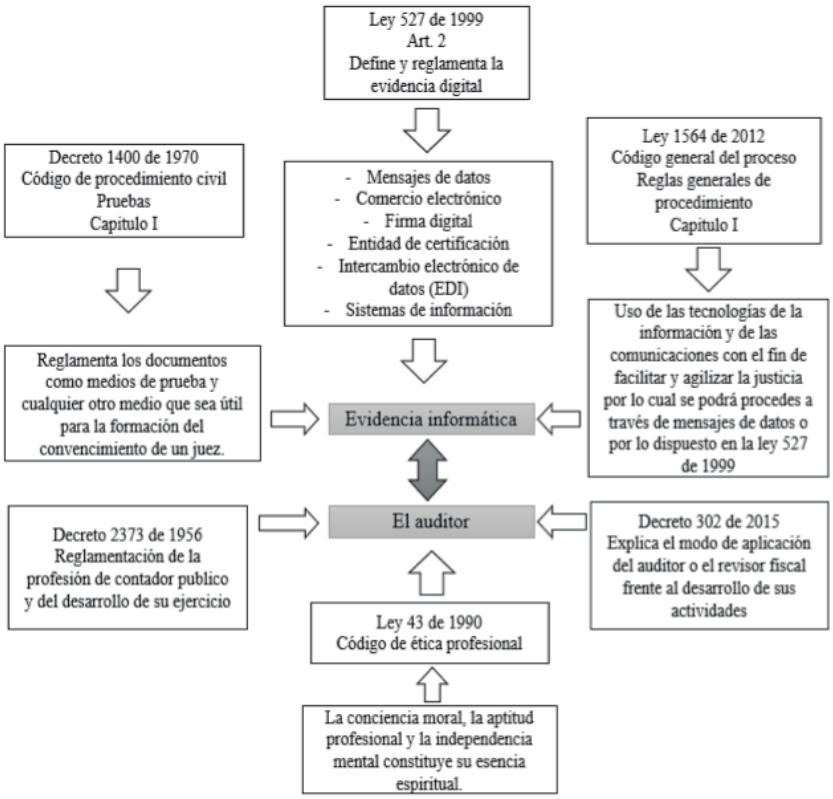
*Fuente. Elaboración propia*

## LA EVIDENCIA INFORMÁTICA DESDE EL PUNTO DE VISTA LEGAL

La evidencia informática ha evolucionado a través del tiempo, esto dado a la necesidad de surgir en el mundo de la economía internacional y de obtener agilidad en procesos financieros, judiciales, tecnológicos, entre otros. Por lo tanto, en este caso el marco jurídico que acobija al profesional auditor, contador o revisor fiscal, se ve obligado a implementar entes de control que determinen nuevas normas, técnicas, leyes, etc. que comprometan al auditor en el desarrollo de su ejercicio, a realizar un trabajo integro, fiable, contundente, veraz, objetivo y sobretodo un desarrollo laboral que genere fe pública ante una sociedad.

A partir del código general del proceso en su capítulo I donde estipula el manejo de la información en la parte informática y electrónica para que por parte de la justicia se agilice y facilite los procedimientos en cuanto a la comunicación de la conceptualización de datos, por lo que permite regular a su vez la evidencia digital. En la siguiente figura vemos la evolución que ha tenido la evidencia informática a través del tiempo.

*Figura 1. Punto de vista legal de la evidencia informática*




*Fuente. Elaboración propia*

La evidencia informática es el elemento clave para corroborar y soportar la opinión del auditor y el resultado final del proceso de auditoría, la evidencia registra los argumentos necesarios para respaldar el informe de auditoría y con este el análisis e interpretación de los hechos vinculados en está para la toma de decisiones.

Como evidencia informática se percibe que son datos digitales que se encuentran almacenados o han sido transmitidos mediante equipos informáticos. Los ordenadores registran toda la actividad que se realiza. Estos registros son fundamentales en las investigaciones informáticas, siempre que se pueda comprobar que no han sido manipulados.

Las evidencias informáticas pueden ser recolectadas por medio de técnicas especializadas por un perito en una investigación informática siempre y cuando estas cumplan de acuerdo a la normatividad jurídica de evidencia digital.

De acuerdo a la ley 1314 de 2009, reglamentada por el decreto nacional 1851 de 2013 y el decreto nacional 302 de 2015 en su Artículo 5°. "Se entiende por normas de aseguramiento de información el sistema compuesto por principios, conceptos, técnicas, interpretaciones y guías, que regulan las calidades personales, el comportamiento, la ejecución del trabajo y los informes de un trabajo de aseguramiento de información" (Ley 1314 de 2009).

La ley 1314 de 2009, expedida por el Congreso de la República, busca apoyar la internacionalización de las relaciones económicas dirigiéndose hacia la convergencia con los estándares de aceptación mundial. Esto con el objeto de obtener participación en la economía global y vinculación en los mercados internacionales, por lo tanto es de vital importancia limitar la libertad económica, mediante normas, técnicas y medidas de aseguramiento de la información que permiten obtener un control y un estándar de auditoria internacional sobre la información financiera.

Las normas internacionales de auditoria (NIA) contienen principios y procedimientos básicos y esenciales para el auditor. Estos deberán ser interpretados en el contexto de la aplicación en el momento de la auditoria, haciendo un énfasis en el análisis de la evidencia informática y las competencias del auditor, basado en la NIA 200, que contiene los objetivos globales del auditor independiente y la NIA 500, que resalta la evidencia de auditoria en una auditoria a los estados financieros.

Aob auditores, explica que la Norma Internacional de Auditoria 200 determina "las

responsabilidades globales que tiene el auditor independiente y establece los objetivos globales del auditor independiente y explica la naturaleza y el alcance de una auditoria diseñada para permitir al auditor independiente alcanzar dichos objetivos."

Por lo anterior se entiende que el auditor será una persona íntegra con independencia mental, capaz de trazar objetivos globales y generar cumplimiento a estos; la norma internacional de auditoria 200 al definir el perfil del auditor, genera confianza para el buen desarrollo de marco normativo, de aquellos procesos y procedimientos que se reflejan en la NIA 500 evidencia de auditoria; evidencia que según García (2014), define como: "La evidencia de auditoría es necesaria para sustentar la opinión y el informe de auditoría. Es de naturaleza acumulativa y se obtiene principalmente de la aplicación de procedimientos de auditoría en el transcurso de la misma."



## RESULTADOS

### ¿Cuáles son los riesgos del auditor y de la recopilación de la evidencia de la información, en el desarrollo de la auditoria informática?

La gestión de riesgos se define como "el conjunto de procesos desarrollados por una organización con el fin de disminuir la probabilidad y ocurrencia de amenazas y de aumentar la probabilidad y ocurrencia de oportunidades con efectos negativos" (Chicano, 2014, p.98). La gestión del riesgo se trata de una metodología o un conjunto de metodologías direccionadas a gestionar correctamente las incertidumbres de una amenaza a las que el contador público en su rol de auditor se enfrenta en el desarrollo de su profesión y deberá valorar mediante la identificación, análisis y evaluación del riesgo.

### Riesgos del auditor frente a la auditoria informática

Moreno y Ramos (2014), definen que los auditores informáticos son personas en las que es característico un amplio bagaje en el ámbito de la informática, son metódicos y se caracterizan por su capacidad de observación y sentido común. Por lo que dichas habilidades deberán ser fuente rigurosa de control para no caer en los siguientes riesgos q invaden el desarrollo profesional del auditor:

Propio interés: Este riesgo existirá cuando al auditor se le presenten conflictos de tipo económico, o de otro tipo, que puedan influir negativamente sobre su

objetividad, provocando una disminución en el rigor de su trabajo con la esperanza de mantener o incrementar el favor de la entidad que audita.

Defensa: La objetividad del auditor podría verse afectada si actuara como defensor de (o en contra de) la posición de su cliente en un proceso o situación antagónica.

Familiaridad o confianza: Existe el riesgo de que el auditor llegue a estar muy influenciado por las cualidades y personalidad del cliente y, por tanto, demasiado de acuerdo con los intereses de este último, depositando una confianza excesiva en sus representaciones y, consecuentemente, reduciendo el alcance de los procedimientos realizados por debajo de los límites requeridos por las Normas de Auditoría.

El riesgo o amenaza de la auto-revisión: La amenaza genérica de la auto-revisión es, depositar una confianza excesiva en el trabajo anteriormente realizado por el mismo auditor que pueda ocasionar el no detectar errores significativos.

La amenaza o riesgo de intimidación: La objetividad del auditor podría verse afectada ante intentos de intimidación provenientes de amenazas u otras presiones, reales o aparentes, por parte del cliente o de un asociado al cliente o por algún otro tercero con poder suficiente. Las consecuencias de estos riesgos o amenazas sobre la independencia del auditor es que puedan reducir la probabilidad de que el auditor quiera detectar los errores e irregularidades existentes y la probabilidad de que comunique los detectados.

## Riesgos de la auditoria en la evidencia informática

El objetivo general del análisis de riesgos es identificar las causas de los riesgos potenciales, en una determinada área y cuantificarlos para que la gerencia pueda tener información suficiente al respecto y optar por el diseño e implementación de los controles correspondientes a fin de minimizar los efectos de las causas de los riegos, en los diferentes puntos de análisis.

En los sistemas informáticos, se pueden señalar las siguientes amenazas o riesgos:

Errores de los usuarios: se considera que este tipo de amenaza llegue a presentarse frecuentemente debido a que los usuarios o el personal nuevo no es capacitado adecuadamente en el uso de los activos “aplicaciones informáticas”.

Modificación de la información: afectará directamente la dimensión de integridad,

porque de presentarse ataques de modificación de información se van a ver alterados los datos almacenados, causando un caos informático y arrojando datos erróneos a la hora de consultas y transacciones en cada uno de los procesos diarios de la institución.

Programas maliciosos: programas destinados a perjudicar o hacer uso ilícito de los recursos del sistema. Es instalado por inatención o maldad en el ordenador abriendo una puerta a intrusos o bien modificando datos. Estos programas pueden ser un virus informático, un gusano informático, un troyano, una bomba lógica o un programa de espía o spyware.

Un intruso: persona que consigue acceder a los datos o programas de los cuales no tiene acceso permitido (cracker, defacer, scrpt boy, viruxer, entre otros.)

Un siniestro (robo, incendio, inundación): una mala manipulación o una mal intención derivan a la pérdida del material o de los archivos informáticos.

Avería de origen físico o lógico: se considera que afecta la disponibilidad porque, las zonas (lugares) donde se han ubicado no son los más adecuados físicamente para su protección o por el contrario el proceso de instalación y/o configuración no fue el adecuado por mala manipulación.

A continuación, se valoran los riesgos de acuerdo al Estándar muy alto, alto, mediano y bajo, teniendo en cuenta los riesgos del auditor y los riesgos en la evidencia informática

## Figura 2. Matriz De Riesgo

| VALORACION DEL RIESGO | FRECUENCIA DEL RIESGO |
|---|---|
| Muy Alto | Muy Frecuente |
| Alto | Frecuente |
| Mediano | Normal |
| Bajo | Poco Frecuente |

| | | RIESGO | DESCRIPCION | PROBABILIDAD | NIVEL DE RIESGO | SUGERENCIA | NORMATIVIDAD | |
|---|---|---|---|---|---|---|---|---|
| RIESGOS DEL AUDITOR | INDEPENDENCIA MENTAL | PROPIO INTERES | Se presenta cuando el auditor o los familiares cercanos tiene intereses financieros u otros en relacion a la entidad auditada. Ejemplo, obtener acciones en la entidad, obtener negocios con el cliente, obtener un potencial empleo con el cliente entre otros. | Poco Frecuente | Muy Alto | Disponer de interes financiero directo. | NIA 200 NIA 210 NIA 220 NIA 240 NIA 260 NIA 710 | Codigo de etica para contadores profesionales Parte A, B Y C. |
| | | | | | | Disponer del interés financiero indirecto en total o disponer de una cantidad suficiente de tal modo que el interés remanente ya no sea de importancia. | | |
| | | | | | | Retirar al miembro del equipo de auditoría. | | |
| | | DEFENSA | Se produce cuando el auditor apoya una posicion hasta tal punto que su objetividad pueda verse comprometida. Ejemplo, cuando el auditor actua en defensa del cliente en un litigio o disputa. | Poco Frecuente | Muy Alto | Ejecutar políticas y procedimientos que prohiban a los auditores que asistan al cliente de auditoría de tomar decisiones gerenciales en nombre del cliente. | | |
| | | | | | | Utilizar profesionales totalmente independientes de los miembros del equipo de auditoria para que lleven acabo el servicio. | | |
| | | FAMILIARIDAD O CONFIANZA | Es manifestada cuando el auditor fruto de una relacion cercana o de otro tipo puede ver comprometida su objetividad. Ejemplo, una relacion familiar directa o indirecta con el cliente o socio, aceptacion de obsequios, etc. | Poco Frecuente | Muy Alto | Retirar al individuo del equipo de auditoría. | | |
| | | | | | | Estructurar las responsabilidad del equipo auditor de modo que este profesional no este involucrado en asuntos que esten acargo de la persona cercana o familiar. | | |
| | | AUTO-REVISION | Se produce cuando un juicio u opinion anterior de un auditor vuelve a ser reevaluada. Ejemplo, que el miembro del equipo de auditoría sea o halla sido directivo de la entidad auditada. | Poco Frecuente | Muy Alto | Seguimiento y monitoria al sistema de control interno. | | |
| | | | | | | Que el cliente sea responsable de la operativa de los sistemas de informacion y de los datos utilizados o generados por el sistema. | | |
| | | | | | | Asignacion de un equipo de auditoría distinto al que participo en el trabajo anterior. | | |
| | | INTIMIDACION | Es causado cuando el cliente amenaza al auditor hasta el punto que este puede ver comprometida su objetividad. Ejemplo, revocacion del mandato o reduccion de los honorarios por su trabjo. | Poco Frecuente | Muy Alto | Revelar al comité de auditoría o a los miembros del Órgano de Administración la extensión y naturaleza del litigio. | | |
| | | | | Poco Frecuente | Muy Alto | Involucrar un auditor adicional que no haya sido un miembro del equipo que originó el litigio, para revisar el trabajo hecho y asesorar en lo que sea necesario. | | |
| RIESGOS EN LA EVIDENCIA INFORMATICA | HUMANOS | ERRORES DE LOS USUARIOS | Se genera cuando el personal no se encuentra altamente capacitado para el manejo de las plataformas o aplicaciones informaticas | Frecuente | Alto | Los funcionarios y/o usuarios que hagan uso de la red de datos de la Institución deberán ser capacitados en temas básicos de seguridad de la información y específicos de acuerdo al área o función encomendada. | NIA 315 NIA 330 NIA 450 NIA 500 NIA 501 NIA 505 | Ley 1273 de 15 de enero de 2009, "De la protección de la información y de los datos" |
| | | ERRORES DE CONFIGURACION | Se origina debido a una mala configuraicon en los activos pertenecientes a las aplicaciones informaticas, llevaria a ataques como intrusion, denegacion de servicios, robo de informacion, etc. | Poco Frecuente | Alto | Se efectuaran copias de respaldo o back-up como salvaguarda de información crítica de los procesos institucionales significativos, la realización de copias de respaldo o seguridad se harán periódicamente en los equipos administrativos y servidores. | | |
| | | MODIFICACION DE LA INFORMACION | Se ocasiona al presentarse ataques de modificacion de informacion alterando los datos almacenados, generando alteracion de informacion e inseguridad en los datos. | Frecuente | Alto | Se documentará detalladamente cualquier novedad que conduzca a poner en riesgo la seguridad de la información, posteriora la revisión de logo registros del sistema con el propósito de analizar la situación y crear o modificar controles en pro del aseguramiento informático. | | |
| | PROGRAMAS MALICIOSOS | VIRUS INFORMATICO | Software malicioso que se diseñan para dañar el equipo al que acceden provocando el borrado de archivos o incluso del sistema operativo al completo. | Normal | Mediano | Para prevenir infecciones de virus informático, los usuarios, no deben hacer uso de software que no haya sido proporcionado y validado por la oficina de TICS. | | |
| | | TROYANOS | Los troyanos son aplicaciones que contienen funcionalidades ocultas con finalidades maliciosas para el usuario. Su modo de acceso es a través de aplicaciones inofensivas que incitan al usuario a ejecutarlo y provocan daños inmediatos o aplazados, como el borrado de datos, la instalación de más programas maliciosos, etc. | Normal | Mediano | El área de TICo jefe a área deberá proporcionar software de protección como antivirus, antimalware y/o seguridad perimetral (firewall) para protección de la información manipulada y almacenada en los equipos de cómputo y servidores. | | |
| | | GUSANOS | Son programas maliciosos autocontenidos cuya finalidad principal es su propagación a otros sistemas para mermar su rendimiento. | Normal | Mediano | En el caso de sospecha de infección de virus, debe dejar de usar inmediatamente el equipo y notificar la sospecha a la oficina de TICS. | | |
| | SINIESTROS | INCENDIO | Al llegarse a presentar fuego como desastre natural se perderia todo el equipamiento informático, acabando con las bases de datos. | Poco Frecuente | Muy Alto | El equipo debe estar ubicado o protegido para reducir los riesgos de las amenazas y peligros ambientales, y el cableado de la energía de las telecomunicaciones que llevan datos o sostienen los servicios de información deben ser protegidos de la intercepción o daño. | | |
| | | AVERIA DE ORIGEN FISICO O LOGICO | Se produce al encontrar los equipos informaticos conectados a fuentes de energia insuficientes, por que los equipos informaticos no cuentan con las condiciones rigurosas de proteccion, etc. | Poco Frecuente | Alto | El administrador del sistema de incidencias (atención a usuarios) deberá priorizar las solicitudes y asignar el personal adecuado para dar solución a los problemas en los puestos de trabajo. | | |

*Fuente: Elaboración propiaw*

## Análisis del procedimiento para la obtención, análisis y presentación de evidencia informática

El auditor frente a la recolección de la evidencia informática en una auditoria determina si el proceso adecuado al inspeccionar, recoger, agrupar, establecer, verificar y evaluar si el sistema informatizado utilizado en una entidad es el más apropiado con respecto al mantenimiento eficaz de los fines de la organización, la integración de la información, salvaguarda los activos y a su vez realiza una utilización de los recursos apropiadamente.

Otro rasgo muy proporcionado frente a esto es la responsabilidad que compete en los determinados momentos de tiempo con el manejo de controles y procedimientos informáticos basados con las técnicas mecanizadas de auditoria, y sumado a ello la valoración al uso del software. Además hoy en día es muy complejo verificar toda la información manualmente ya que son miles de procedimientos los que se utilizan en las entidades y con ello se restringe la facilidad de obtener un resumen, calcular y clasificar datos, por ello se debe implementar software de auditorías o en su caso las técnicas asistidas por computadora. Sánchez (s.f)

Detro de la recolección de la información para cuantificar o cualificar la evidencia informática y hacer buena destinación de la auditoria es necesario manifestar la importancia que presenta la información para ello, Rodríguez (1996) define lo siguiente “La información es un bien que tiene unas características determinadas y determinantes es, no cabe duda, un bien económico, pero diferente a los demás bienes económicos existentes en un mercado tradicional” en consonancia certifica el claro modelo de que se trata como un bien que no se agota con el consumo, puede ser utilizados por miles de personas y como resultado nos ayuda a fortalecer diferentes ítems de conocimiento.

Teniendo claro el concepto anterior, se analiza la importancia que la información tiene en un encargo de auditoria y para ello en el Código de Procedimiento Civil en el art 175 “Medios de prueba. Sirven como pruebas, la declaración de parte, el juramento, el testimonio de terceros, el dictamen pericial, la inspección judicial, los documentos, los indicios y cualesquiera otros medios que sean útiles para la formación del convencimiento del juez”. Lo anteriormente mencionado, resalta que la información puede ser obtenida de distintas maneras y servir de punto de partida para llevar acabo procesos pertinentes en la sociedad.

En este contexto, al presentar una evidencia informática dentro de la recolección de datos se verifica en el código de procedimiento civil en su art 251 que la presentación pude darse con “Distintas clases de documentos. Son documentos los escritos, impresos, planos, dibujos, cuadros, fotografías, cintas cinematográficas, discos, grabaciones magnetofónicas, radiografías, talones, contraseñas, cupones, etiquetas, sellos y, en general, todo objeto mueble que tenga carácter representativo o declarativo, y las inscripciones en lápidas, monumentos, edificios o similares” lo que quiere decir que dentro de la auditoria a la parte informática del ente se realiza por medio de cuestionarios, entrevistas, software de auditoria y las TAC y de allí la información obtenida se recolecta como mejor se facilite.

Depués de obtenida la información en el medio correspondiente el auditor informático debe de realizar una labor eficaz y a la vez evita situaciones desagradables por lo que le concierne conocer la rama de derecho, dichas circunstancias se presentan en el entorno en que trabaja, por lo que en este caso equipararemos puntos específicos para el desarrollo de tal presentación y su organización.

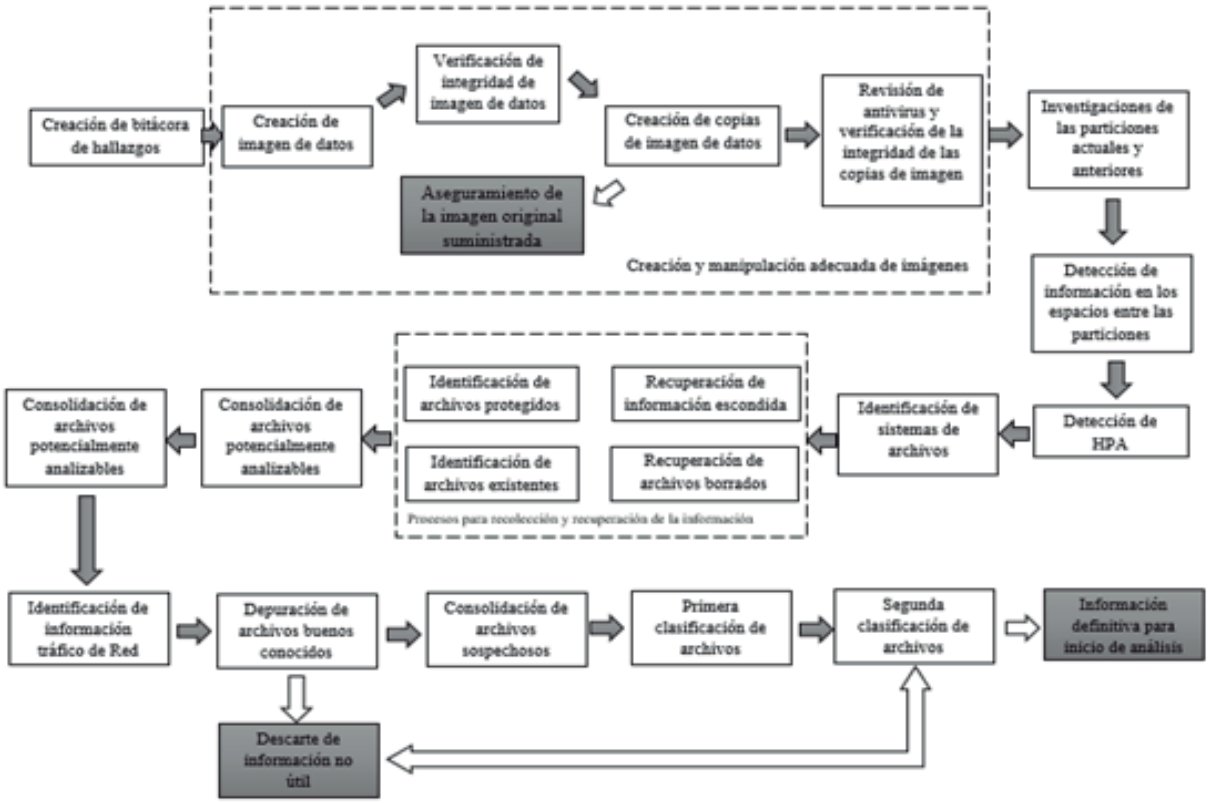
En la Constitución Política de Colombia en su art 61 dice “El Estado protegerá la propiedad intelectual por el tiempo y mediante las formalidades que establezca la ley”. Para lo que concierna sobre los derechos de autor y su finalidad dentro de lo que ejecuta la persona dentro de las creaciones de intelecto.

Las ISACA son normas especializadas que divulgan la figura frente al manejo de la auditoria de sistemas de información y le permiten al auditor informarse de los sucesos más pertinentes frente a sus responsabilidades sujetas en el Código de Ética Profesional y dentro de desarrollo de sus actividades competentes en el trabajo que ejecuta permitiendo a su vez desarrollar eficazmente el trabajo de auditoria a plantear y la forma de obtención de la evidencia.

Las NIAS son normas que especifican el desarrollo de la auditoria y pertinentes a ellas se desenlazan toda la clasificación frente a desarrollo de la planeación y ejecución de la auditoria todo ello inmerso en la NIA 300 y frente a la obtención de la evidencia tema particular en este artículo se encuentra en la NIA 500 y 501 donde nos describe toda la particularidad que se tiene en el tema.

Frente a todo lo diserto frente a la evidencia informática la siguiente figura es un claro ejemplo de la manera en cómo se obtiene la evidencia a partir de la información y su gran valor.

*Figura 3. Diagrama de examinación y recolección de Datos*




*Fuente: Mintic. Manual de Manejo de Evidencias Digitales y Entornos Informáticos versión 2.0*

En la figura 3. Diagrama de examinación y recolección de Datos, define como el contador público en su rol como auditor realiza una planeación adecuada y preferente para socializarla por medio de la manipulación informática, después ejecutarla y por ende realizar un informe a su criterio desde su juicio profesional.

El principal elemento de la planeación de la auditoria relacionada con la informática se encuentra de la mano con la NIA 300 que es la que refiere la estrategia básica frente a las actividades que se realizaran en la auditoria, donde el primer paso es la obtención de información general de la organización y sobre la información informática a evaluar sobre los sistemas, procedimientos y los equipos de cómputo.

La NIA 200 en efecto dirige las responsabilidades globales del auditor independiente donde lleva a verificar el alcance y cumplimiento de los objetivos de la auditoria por lo que de eso se despliega las habilidades especializadas que es la ayuda de un profesional siendo el caso del uso del trabajo de un experto, para fines de la auditoria

según las NIAS.

La planeación se relaciona a tres puntos específicos que son desde la alta dirección, la auditoria y la informática donde varía desde la importancia que cada uno de estos tiene para el desarrollo de las actividades frente a la investigación preliminar a solicitud de cumplimiento de políticas, manuales, estatutos entre otros, como procedimientos de auditoria y la tecnología manejada en el ente y sus diferentes controles.

La ejecución dimensiona cada punto anterior, donde el desarrollo consiste en desarrollar el programa de trabajo teniendo en cuenta el tiempo, el costo, el personal a necesitar, los documentos auxiliares y las entrevistas previas, esta a su vez se encarga de facilitar la elaboración de los cuestionarios, realizando también una documentación narrativa y la revisión y evaluación de controles

El informe se realizará con evidencia suficiente y adecuada recolectadas en el proceso de la ejecución de la auditoria donde se tendrá en cuenta la NIA 500 sobre la evidencia esta estará sujeta en los cuestionarios, en la documentación narrativa, en CD, en USB y grabadora de voz donde estarán los hallazgos, partiendo de esto se realizara el informe y para el desarrollo de este encontramos la NIA 705 que refiere a emitir un informe adecuado, después de entregado el informe se llevara un seguimiento bimestral, trimestral o semestral puesto que las software tienen cambios mayores frente a la tecnología.

Las técnicas de auditoria asistidas por computador sientan el desarrollo de la auditoria para la recolección de la evidencia informática estas manifiestan la utilización de software genérico de auditoria, genera datos de prueba y realiza técnicas de pruebas integradas como base para la recolección de auditoria.

## La evidencia informática del perito contable en el proceso judicial

Normalmente la auditoria informática se aplica de dos formas distintas; por un lado, se auditan las principales áreas del departamento de informática: explotación, dirección, metodología de desarrollo, sistema operativo, telecomunicaciones, bases de datos, etc.; y por otro, se auditan las aplicaciones (desarrolladas internamente, subcontratadas o adquiridas) que funcionan en la empresa.

En Colombia los campos o departamentos de informática más vulnerables son los sistemas operativos y las bases de datos, los cuales se encuentran contemplados en

la ley 1273 del 5 de enero de 2009, como uno de los distintos medios para ocasionar un delito informático. Dado al imparable avance tecnológico y a los distintos conocimientos que desarrollan diferentes individuos sobre el ámbito tecnológico, y que desafortunadamente no siempre dicho conocimiento se aplica al margen de un marco legal. Surge la necesidad de combatir las causales de delitos informáticos, de acuerdo, al marco legal normativo que sea aplicable y bajo la jurisdicción de un personal altamente capacitado para auditar y obtener la debida evidencia suficiente y probatoria (perito informático).

Por lo anterior, se contempla el código de procedimiento penal en su artículo 233 (medios de prueba), se consagra la peritación como evidencia suficiente y probatoria para uso judicial. Ahora bien, el perito deberá tener título oficial en la ciencia o arte al que pertenezca el punto sobre el que han de dar su dictamen, esto con el fin de que evidencia hallada en el proceso pericial refleje un convencimiento de la verdad o certeza de un hecho o afirmación fáctica para fijarlos como ciertos a los efectos de un proceso.

A continuación, se citaran diferentes casos de delitos informáticos donde se analizara la diferente evidencia informática suficiente y probatoria, ante los diferentes procesos judiciales a enunciar:

*Tabla 1. Caracterizar los mecanismos de control*

| Caso | Sentencia Y/U Otro | Delito | Evidencia | Norma |
|---|---|---|---|---|
| Jorge Maximiliano Pachón Viola | AP1916-2017 RAD. 49747 | Hurto por medios informáticos y acceso abusivo a un sistema informático. | Documentos fílmicos tomados por las cámaras de seguridad de Bancolombia y microfilmadoras. | Código Penal Arts. 269A Y 269I. |
| Carlos Arturo Álvarez Trujillo | SP1245-2015 | Hurto por medios informáticos y semejantes, concierto para delinquir y falsedad en documento privado | Computadores, bases de datos, y material físico. | Código Penal Arts. 269I, 340 Y 289. |
| Hacker Andrés Sepúlveda | Editorial el Tiempo | Concierto para delinquir, acceso abusivo informático, uso de software malicioso y violación de datos personales. | Ocho computadores, varias USB, documentos de la Fuerza Pública, listados de desmovilizados de la guerrilla y reportes sobre campañas políticas. | Código Penal Arts. 269A, 269C, 269E Y 269F. |
| Hacker Juan Esteban Ramírez Gil | Editorial el Tiempo | Acceso abusivo a un sistema informático y daño informático. | Discos duros, dispositivos USB y un amplificador de red. | Código Penal Arts. 269A Y 269D |

*Fuente: Departamento Administrativo de la función pública. Sentencias Judiciales. Editorial el Tiempo*

Los anteriores casos expuestos, en similitud, son infractores de la ley 1273 de 2009 “de la protección de la información y de los datos”, los acontecimientos presentados reflejan los diferentes delitos informáticos cometidos.

## CONCLUSIONES

El auditor informático en su experticia como indagador se proyecta a evaluar y ordenar una serie de actividades donde destaca el riesgo que contrae como auditor y mediante la revisión de la documentación de los cuales estudia sus probabilidades y de la misma manera da una sugerencia si llegado el caso esta se presenta para ello pone en práctica todos sus conocimientos y trabaja bajo sus técnicas.

La evidencia informática se obtiene de la planeación ejecución e informe que el auditor realizara después de haber puesto en práctica sus papeles de trabajo dentro de los cuales pone en práctica las TAC que permitirán obtener una evidencia por medio de la revisión del software por lo que verificara la planificación estratégica, administrativa, y técnica soportada en documentos, grabaciones, archivos en USB.

El perito no nace: se hace, con formación específica. Efectivamente se concluye que un perito, lo es en tanto a unos conocimientos y una experiencia específica en el ámbito profesional, de la cual depende la claridad y objetividad de la evidencia para la presentación del dictamen pericial.

## REFERENCIAS BIBLIOGRÁFICAS

Alvarado, R. M. (2004). La independencia del auditor en la Unión Europea.. Madrid, ES: Dykinson. Retrieved from http://www.ebrary.com

Blanco, E. L. J. (2005). Auditoría y sistemas informáticos. La Habana, CU: Editorial Félix Varela. Retrieved from http://www.ebrary.com

Chicano, T. E. (2014). Auditoría de seguridad informática (MF0487_3). Madrid, ESPAÑA: IC Editorial. Retrieved from http://www.ebrary.com

Davara, R.M.A. (1996) De las autopistas de la información a la sociedad virtual. Aranzadi, Pamplona

Derrien, Y. (2009). Técnicas de la auditoría informática. Barcelona, ES: Marcombo. Retrieved from http://www.ebrary.com

Moreno, P. J. C., & Ramos, P. A. F. (2014). Administración de software de un sistema informático. Madrid, ES: RA-MA Editorial. Retrieved from http://www.ebrary.com

Piatiini, M.G. (s.f) Auditoria Informática, un enfoque práctico. 2° Edición ampliada y revisada

Sánchez-Toledo, L. A. (2009). Guía para la auditoría de los sistemas de gestión de la seguridad y salud en el trabajo. Madrid, ES: AENOR - Asociación Española de Normalización y Certificación. Retrieved from http://www.ebrary.com

## LEYES Y JURISPRUDENCIA

Asamblea Nacional Constituyente. (1991). Constitución Política de Colombia. Bogotá: Legis.

Congreso de la República de Colombia. (30 de diciembre de 1960). Ley 145 de 1960. Por la cual se reglamenta el ejercicio de la profesión de contador público. Diario Oficial 30433 del 3 de febrero de 1961. Recuperado de goo.gl/jNWuDI

Congreso de la República de Colombia (13 de diciembre de 1990). Ley 43 de 1990. Por la cual se adiciona la Ley 145 de 1960, reglamentaria de la profesión de contador

público, y se dictan otras disposiciones. iario Oficial 39602 del 13 de diciembre de 1990. Recuperado de goo.gl/iN0RRE

Congreso de la República de Colombia. (31 de agosto de 2004). Ley 906 de 2004. Por la cual se expide el Código de Procedimiento Penal. (Corregida de conformidad con el Decreto 2770 de 2004). Diario Oficial 45658 del 1.o septiembre de 2004. Recuperado de goo.gl/ZPPkbx

Congreso de la República de Colombia (13 de julio de 2009). Ley 1314 de 2009. Por la cual se regulan los principios y normas de contabilidad e información financiera y de aseguramiento de información aceptados en Colombia, se señalan las autoridades competentes, el procedimiento para su expedición y se determinan las entidades responsables de vigilar su cumplimiento. Diario Oficial 47.409 del 13 julio de 2009. Recuperado de goo.gl/9LRRHS

Congreso de la República de Colombia. (12 de julio de 2012). Ley 1564 de 2012. Por medio de la cual se expide el Código General del Proceso y se dictan otras disposiciones. Diario Oficial 48489 del 12 julio de 2012. Recuperado de goo.gl/kXpwJd

Decreto 2420 de 2015. Por medio del cual se expide el Decreto Único Reglamentario de las Normas de Contabilidad, de Información Financiera y de Aseguramiento de la Información y se dictan otras disposiciones". Diario Oficial No. 49.726 de 14 de diciembre de 2015. Recuperado de https://www.cancilleria. gov.co/sites/default/files/Normograma/docs/decreto_2420_2015.htm

Ley 527 de 1999 (agosto 18). Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones. Diario Oficial No. 43.673, de 21 de agosto de 1999.

Manual de Manejo de Evidencias Digitales y Entornos Informáticos versión 2.0. Texto refundido de la Ley de la propiedad intelectual, título VII del libro, art 95 la protección de los programas de computador