International Journal of Scientific Research and Engineering Development-– Volume 5 Issue 4, July-August 2022

Available at www.ijsred.com

RESEARCH ARTICLE OPEN ACCESS

Accounting and Financial Auditing: The Extraction of Digital Evidence as a Mechanism to Ensure the Chain of Custody

Naydù Judith Jàcome Castilla[*], Erwin Hernando Jàcome Castilla**, Eduardo Luis Jàcome Castilla[***]

*(ROT Aresearchgroup, Universidad Francisco de Paula Santander Ocaña, Colombia
Email: njjacomec@ufpso.edu.co)

** (ApirakunaResearchGroup, Universidad Francisco de Paula Santander Cúcuta, Colombia,
Email: erwinhernandojc@ufps.edu.co)

*** (GEDES researchgroup, Universidad Francisco de Paula Santander Cúcuta, Colombia,
Email: eduardoluisjc@ufps.edu.co)

----------**********----------

Abstract:

The article presents the results from the theoretical approach of a research process that characterized the accounting and financial auditing processes, to achieve the assurance of the chain of custody in the extraction of digital evidence through the application of forensic analysis. As a method of study, descriptive research of documentary type was used, with secondary sources of information, from the theory of accounting and financial auditing that adjusted to the current legal regulations served to establish the necessary tools of information security, in the extraction of digital evidence and the anchoring of the chain of custody. As a contribution to the theoretical concepts of information security, the audit procedures, the laws in force and the software characteristics that the systems must contain in terms of usability and applicability were compiled.

Keywords **—audit, chain of custody, evidence, standardization, standardization**

----------**********----------

I. INTRODUCTION

The research presents a theoretical approach for the assurance of the chain of custody and the extraction of digital evidence from an information system in an accounting and financial audit; taking into account this, from the theories of forensic analysis, the adequate and suitable conditions were established to preserve the information collected in an accounting and financial audit process, given that currently the accounting and financial systems of the organizations are in a computer system, which can be altered before or after the accounting and financial audit is carried out.

The research process proposed a tool, focusing its study on the adequacy in the accounting and financial auditing processes of business organizations, taking into account that 23.6% of the productivity of companies are related to the engineering area. [1]. In this sense, by means of forensic techniques, the relevant tools were characterized to guide the audit for the preparation, analysis and presentation of digital evidence in the reports generated by the auditor; so that the information system has the principles and constitute a means of proof in an audit process.

According to the above, the development of the study was characterized purpose, functionality and legal requirements of an accounting and financial audit; this in order to establish the audit procedures and current regulations for the extraction of digital evidence and the preservation of the chain of custody, then the necessary software tools to be

used for information security were established, structuring the technical requirements to be used.

Thus, as a result of the research, it was possible to systematize the necessary tools regarding the legal and technical requirements for an accounting and financial audit of a business organization's information system.

II. METHODOLOGY

The methodological design of a research process according to. [2] "allows the recording, analysis and interpretation of the actual nature of a fact or phenomenon", in such sense the research is descriptive, characterizing the theoretical and legal foundations of accounting and forensic auditing, as it states [3] In this sense, the research is descriptive, characterizing the theoretical and legal foundations of accounting and forensic auditing, as it is stated, specifying that the level of research depends on the degree of depth and the way of approaching the subject. At the same time, a documentary and applied research was established. [4] In turn, a documentary and applied research was established, characterizing the procedural and legal conditions that accounting and forensic audits must contain with the objective of establishing the tool that allows the information system to constitute working papers and means of proof in an audit report.

Based on the objectives set and the methodology designed, for the development of the research, the main theoretical references taken as main theoretical references were the contributions made by [5] in terms of forensic auditing and how entities with access with access to new technologies have seen the need to improve their information systems, through control mechanisms with the application of the processes of forensic auditing, providing concepts related to forensic auditing that professionals who perform audits are due to minimize the vulnerability of an information system.

Regarding the characterization of the accounting and financial audit process, we used the concepts of [2], related to forensic auditing and accounting practices in criminal investigation and money laundering. Regarding the legal requirements in terms of computer crimes, securing digital evidence the contributions of [3]The law on computer crimes was elaborated by the law firm, who in turn contemplated the contributions in software of [4]. Following in this context, each one of the variables of the investigation was processed to determine the suitability in the accounting and financial audit.

III. RESULTS

In systems auditing processes, computer experts look for the traces reflected in the use of an information system, according to [9]"previous research has recognized the importance and scope of ICT goods and services to improve organizational processes" is how, in the case of an accounting and financial audit, information systems constitute the evidence in the accounting and financial processes of companies, this is why to preserve the adequacy of the investigation, the characteristics of forensic, accounting and financial audits were established, the regulations concerning computer and financial crimes and the software technology supports necessary to preserve the chain of custody.

A. Characterization of forensic, accounting and financial auditing

In the business world today, organizations, whether large, medium or small, according to the advances in technology, are increasingly using information systems in the development of their daily activities, as stated by [10] The report states that, out of 23,252 companies, 99.5% of industrial and commercial companies use a computer for information storage.

Starting from the premise that companies "are subject primarily to the achievement of their objectives and for compliance it is necessary to raise hybrid strategies for the organization to be effective". [11] and being these systems fed by a set

of data, such as Excel files, access, server database, Oracle that can be altered or modified, by the same DBA Database Administrator or any member of the working group with the same privileges, in the same way they can alter with hacking techniques such as the injection of top 10 owas or black hat hackers who perform these activities for fun or crackers who do it for economic benefit.

In this sense and according to the problems presented in the use of information systems, the leaders of the processes, understood as the people who must "anticipate the facts and act under strategies and actions thought out and appropriate to the environment and the situation presented to them"[12].The engineers in charge of the organizations and the accountants who record and report the accounting and financial information report such eventualities with the purpose of taking preventive measures to minimize the occurrence of these events or corrective measures when during the audits they find findings that indicate that the systems of the companies have been violated; Thus resorting to forensic audit techniques of an information system, being the suitable professionals for the realization of this activity those who have the legal and technical knowledge that give assurance to the organization that the system was not subject to any alteration of the information, in order to safeguard the digital evidence and the chain of custody of the information.

Therefore, for this research it became necessary to establish the differences between what is known as financial auditing in an accounting information system and forensic auditing, establishing how these become transversal tools for the assurance of a company's financial information.

As a first step, according to the studies conducted by financial audit theorists [13]The main objective is the analysis of its operations to determine the result of its financial operations in compliance with the standards required by the accounting and financial law, which in comparison with the forensic audit according to the specialized forensic laboratory [5]The purpose of the forensic audit is to "find, collect and analyze financial, accounting, administrative and legal information present in physical and/or digital documents for legal purposes, which allow to analyze and reconstruct the financial events occurred"; this is how these two types of audits are complementary and necessary for the evidence in case of a legal process, where alterations or modifications of the accounting and financial system of an organization have been committed.

In this sense, the financial audit is carried out by professionals trained in the accounting and financial area who analyze the accounting information in its registration and presentation of financial statements, for which they perform the phases of planning, conducting field work and preparation and issuance of audit reports for which the forensic audit is used, which is responsible for obtaining the records of information systems, with the purpose of serving as a means of proof of the audit and the reports that are generated from these.

B. Characterization of the legal framework for forensic and financial auditing

To perform the forensic audit as a means of evidence when financial auditing processes are carried out, the current regulations must be taken into account regarding the assurance of digital evidence and chain of custody, in case of being a means of evidence in a court case; for example for tax or judicial cases in which the objective is the inspection and surveillance of the state, the authorities and control mechanisms refer to the law of habeas data, only resorting to the mechanisms indicated by law in the request for information making use of the protection of personal data and privacy.

In this order of ideas, the authorities have different mechanisms for the control of fraud in organizations, as stated in the law 527 of 1999 [14]where it was regulated how should be the access and use of data messages, electronic commerce and digital signatures; establishing in those cases how the information should be given

and how the evidence should be contained to be validated by a judge as a means of evidence, stating that for its reliability is given in the terms in which the message was generated and how the integrity of the information was preserved.

Subsequently, with regard to the protection of information and data, Law 1273 of 2009 [15]The law also establishes the actions that constitute a violation of the integrity of information systems, highlighting when access is illegitimate and when it is abusive access, typifying the crimes with the objective of prosecuting the culprits; Also with this law of computer crimes speaks of the originality, integrity, and authenticity being very difficult for the current organizations the application of these legal precepts, is when through the forensic audit and experts related to the subject can be performed in an appropriate way the extraction of evidence in a financial audit process, being essential these tools before a judicial process that is derived from the findings generated in these.

This is how from the conceptualized in the Political Constitution of the Republic of Colombia [16]Article 15 "All persons have the right to their personal and family privacy" and the provisions of the law on computer crimes, a theoretical approach was made to serve as a step-by-step process for a financial audit process to carry out a forensic audit that generates means of proof and preservation of digital evidence.

C. Computer Technology for Accounting and Financial Auditing: A Forensic Analysis Approach

Based on the phases of the financial audit and the needs of the auditor, a professional who must have triadic thinking, i.e. "a logical mind to think, a rational mind to act and an emotional mind to feel", a theoretical approach was designed to guarantee digital evidence and the chain of custody of information.[17]a theoretical approach was designed to guarantee digital evidence and chain of custody of information, considering forensic auditing as the main tool, thus combining the contributions of these two sciences for the effective use of information systems and the success of financial auditing as a mechanism for the prevention and correction of financial computer crimes.

As stated above, from the forensic audit and financial audit for the preservation of digital evidence and chain of custody of information, the theoretical approach was structured according to the phases of the audit, the planning phase and risk assessment with forensic analysis tools as follows:

Planning and risk assessment

Being the planning and risk assessment in the financial audit the first phase, where its main objective is to know the business, its environment, external factors, the accounting regulatory framework, the criteria to be taken into account in the evaluation and measurement of results, determining the possible errors that the auditor can make, at this stage the technique for digital evidence is based on the following steps to be followed in the planning and protocol to follow:

D. Legal regulations and technical requirements for the management of a financial information system as evidence of an accounting and financial audit.

The planning and risk assessment in the audit, so that the digital evidence constitutes a means of proof of the partners of the organizations and / or judges in a judicial process, should be performed as a preventive control of the audit a legal review, against the accounting standards required by the control entities, in turn should be performed a forensic analysis of the systems in terms of accounting and financial packages in which the accounting of the company is recorded, so that through forensic techniques to help the auditor preserve and analyze the digital evidence and the chain of custody as a means of proof.

For this, the audit group should be formed by experts in the financial and accounting area and professional forensic experts in charge of performing a forensic reproduction, by means of a

copy of the digital evidence, so that the system data are not modified; All this with forensic tools such as specialized software and mechanisms for collecting digital evidence, this must be done through a protocol, which is why it is important that in the planning of the audit is prioritized in the need to preserve intact the digital evidence, all this in order to safeguard the reliability of the information obtained to meet the requirements as evidence in the punishment of crimes within an organization. In this process the forensic experts analyze the organization and define the protocols to be followed, the forensic analysis tools to be applied in the audit.

E. Forensic analysis mechanisms to explore the hard disk where the digital evidence is located.

To fulfill this procedure that is performed to the computers where the accounting and financial information is located, it is necessary to establish in the planning protocol, the number of computers that contain the information, the number of users where an overview of the folders and files to be analyzed is obtained, for this can be used SpaceSniffer , Scanner or WinDirStat Portable tools that offer expeditious summaries of the distribution of space on hard drives, this with the purpose of creating a database using getFolder and FileLister. (Softonic, 2015).

F. Digital evidence packaging and securing

In this part of the forensic analysis, once all the information storage equipment has been obtained, a forensic image is made, preparing the forensic equipment where the analysis software has been installed, installing the write blocker and with specialized software the forensic image is made, saving the images obtained on a hard disk, then a copy of the original is made, which is used for the accounting and financial audit.

To obtain the forensic images it is important to use hand tools and personal protection in order to preserve the digital evidence and the security of the forensic expert, this process should be documented by taking photographs where the documents and digital evidence were found, detailing in the report the computers, devices with make and model, taking a photograph of the location of these.

G. Forensic identification in the audit process

This step is one of the most important, it corresponds to obtaining the MD5 HASH, which is nothing more than the digital fingerprint of each of the files to be used in the accounting and financial audit that are stored in a technological storage and constitute working papers in the audit and evidentiary means; the extraction of the MD5 HASH is performed, the next step is the process of packaging the digital evidence, using the copies taken for the audit.

Thus, for financial auditing processes, forensic auditing experts are necessary to determine an adequate process for taking the digital evidence that constitutes the working papers of this audit, which serves as evidence in a process.

IV. CONCLUSIONS

In financial and accounting auditing in organizations, it is necessary to use forensic auditing tools to obtain digital evidence in accounting information systems, for which the most important mechanism is the way in which this information is obtained. It also describes the process of storing and preserving evidence step by step, which helps in the proper execution of a financial auditing process.

It is for this reason that the legal and technical requirements of software with which the audit must be developed from the planning of the audit and its execution in a business organization are described. In this sense it is important to emphasize for the organizations, constituted as small, medium or big companies, the importance in the assurance of the information of their companies, information that many times for not having the suitable protocols does not constitute means of test in a process, it is for this reason that to use the mechanisms of the forensic audit described in the designed technique serve as measure of control so that the information is not altered or violated

REFERENCES

[1] O. Manzano - Durán, M. M. Peñaranda - Peñaranda y J. C. Luna - Quintero, «Sostenibilidad y proyectos sostenibles: Estudio bibliométrico,» *Revista Científica Profundidad Construyendo Futuro,* vol. 14, nº 14, pp. 15-24, 2021.

[2] Pallela y Martins, Metodologia de la Investigación Cualitativa, Caracas: Fedupel, 2006.

[3] F. Arias, El proyecto de Investigación, Caracas: Episteme, 2012.

[4] Sabino, Método de investigación, Caracas: Panapo, 1996.

[5] Adalid, «Adalid,» Marzo 2018. [En línea]. Available: https://www.adalid.com/auditoria-forense/.

[6] Fontan, «Foro de Profesionales Latinoamericanos de seguridad,» 2018. [En línea]. Available: http://www.gestiondelriesgo.com/artic/discipl/4166.htm.

[7] Diaz, Apunt4es de Derecho Informático, Bogotá: Habeas Data Consultores, 2014.

[8] Cano, Computación Forense, descubriendo los ratos informáticos, Bogotá: Alfaomega, 2013.

[9] V. Cruz - Carbonell, Á. F. Hernández - Arias y A. C. Silva - Arias, «Cobertura de las TIC en la educación básica rural y urbana en Colombia,» *Revista Científica Profundidad Construyendo Futuro,* vol. 13, nº 13, pp. 39-48, 2020.

[10] DANE, «Indicadores básicos de TIC en Empresas,» [En línea]. Available: https://www.dane.gov.co/index.php/estadisticas-por-tema/tecnologia-e-innovacion/tecnologias-de-la-informacion-y-las-comunicaciones-tic/indicadores-basicos-de-tic-en-empresas.

[11] C. A. Pacheco - Sánchez y F. Rodríguez – Téllez, «Empresas B: un diagnóstico sobre su aplicabilidad,» *Revista Científica Profundidad Construyendo Futuro,,* vol. 10, nº 10, pp. 2-9, 2019.

[12] Y. González - Castro, O. Manzano - Durán y M. Torres - Zamudio, «Liderazgo: una práctica sistémica en el futuro empresarial,» *Revista Científica Profundidad Construyendo Futuro,* vol. 14, nº 14, pp. 64-72, 2021.

[13] República,C.G., «Guía de auditoría Financiera.Guía de auditoria Financiera. Contraloria General de la Republica de Colombia,» 2017. [En línea]. Available: https://www.contraloria.gov.co/guia-de-auditoria-en-el-marco-de-normas-issai/2.-guia-de-auditoria-financiera.

[14] Senado de Colombia, «Ley 527 de 1999. Bogotá,» 1999. [En línea].

[15] Senado de Colombia, «Ley 1273 de 2009,» 2009. [En línea].

[16] Senado de la Republica, «Constitución Política de Colombia,» 1990. [En línea].

[17] J. A. Lemus - Quintero, «Pensamiento tríadico y su relación con variables sociodemográficas de los estudiantes de Administración de Empresas,» *Revista Científica Profundidad Construyendo Futuro,* vol. 14, nº 14, pp. 54-63, 2021.

