Recibido: 19 – 01 – 2022 / **Aceptado:** 12 – 03 – 2022 / **Publicado:** 12 – 08 – 2022

ARTÍCULO DE INVESTIGACIÓN

Methodological proposal for the generation of supports that supportb the collection of digital evidence, in entities of the financial sector

Propuesta metodológica para la generación de soportes que apoyen la recolección de evidencia digital, en entidades del sector financiero

Camilo Cardona

Cómo citar: ZCardona, C. (2022). Methodological proposal for the generation of supports that support the collection of digital evidence, in entities of the financial sector. Hashtag, (20), 71-82

Abstract

With the development of this article, a methodology is proposed that supports commercial and business processes for companies in the financial sector, as an alternative to face the high rates of cybercrime reported in recent years, ensuring orderly and articulated execution, among the different dependencies, to mitigate the impacts of an attack, in addition to facilitating the identification and collection of digital evidence for forensic investigation processes in cases in which it is demonstrated that an incident has occurred that violates cybersecurity mechanisms, this is a Currently a dominant need, because due to the social changes resulting from the pandemic, more and more people find themselves in need of resorting to digital infrastructures to access financial services and electronic commerce platforms. Based on the analysis and in accordance with the financial context, a review of documents recovered from digital repositories is carried out to identify the main computer infringements related to the materialization of financial crimes. By way of the scientific impact achieved through this research work, a starting point is established through which it is possible to reinforce the computer security of management systems in companies in the financial sector, complementing it with the generation of supports that can be used as digital evidence in an eventual forensic investigation process, it is also evidenced the need to implement a holistic vision in the processes, which allows an efficient response to IT security needs.

Keywords:

Cybercrime, Financial crimes, Digital evidence, Computer forensics, Work methodology

Resumen

Con el desarrollo de este artículo, se propone una metodología que apoye los procesos comerciales y de negocio para las empresas del sector financiero, como alternativa para enfrentar los altos índices de cibercrimen reportados en los últimos años, asegurando una ejecución ordenada y articulada, entre las diferentes dependencias, para mitigar los impactos de un ataque, además de facilitar la identificación y recolección de evidencia digital para procesos de investigación forense en casos en los que se encuentre demostrado que ha ocurrido un incidente que viola los mecanismos de ciberseguridad. Esta es una necesidad actualmente dominante, pues debido a los cambios sociales derivados de la pandemia, cada vez más personas se ven en la necesidad de recurrir a infraestructuras digitales para acceder a servicios financieros y plataformas de comercio electrónico. A partir del análisis y de acuerdo con el contexto financiero, se realiza una revisión de los documentos recuperados de repositorios digitales para identificar las principales infracciones informáticas relacionadas con la materialización de delitos financieros. A través del impacto científico logrado a través de este trabajo de investigación, se establece un punto de partida a través del cual es posible reforzar la seguridad informática de los sistemas de gestión en empresas del sector financiero, complementándolo con la generación de soportes que puedan ser utilizados como evidencia digital en un eventual proceso de investigación forense, también se evidencia la necesidad de implementar una visión holística en los procesos, que permite una respuesta eficiente a las necesidades de seguridad de TI.

Palabras clave:

Cibercrimen, Delitos financieros, Pruebas digitales, Informática forense, Metodología de trabajo

Introduction

In recent years, information and communication technologies have been assimilating more and more aspects within which all human dimensions are developed, at a social, educational, political, labor, economic and financial level, among others, this situation it generates opportunities within cyberspace for criminals, who through deception and exploiting vulnerabilities try to obtain illicit benefits from sometimes unsuspecting and other cautious users. In response, individuals and businesses alike have had to implement protective barriers to help mitigate the degree of exposure.

In particular, companies need to implement robust infrastructures for the protection of technological assets and their clients' information, however, based on the idea that there is no totally reliable system, it is to be understood that at some point, an incident will take place that affects computer security, from that moment on, the priority is to recover the operability of all systems in the shortest possible time, but once the urgency is attended to, companies need to identify those responsible, the tools, the vectors and Any other element that allows a deep understanding of how the attack was perpetrated, that later allows the reconstruction of the chain of events, to prevent it from happening again and to take legal measures if it is the case; All this is possible thanks to the techniques of computer forensics, however in many cases, the information that can be recovered after the attack has occurred is limited, altered or was eliminated; To reduce this scenario, this work addresses a methodology focused on providing a framework that allows the generation of records on the activities carried out by the collaborators of financial entities, focused on the permanent generation of information sources that can serve as evidence. digital.

For the development of this article, an analysis is carried out that allows to know the advances in techniques and models for the collection of evidence in cases related to financial crimes, the methodology used for this investigation is exploratory, not experimental descriptive with cut transversal, since it seeks to investigate the advances and applicability of methods related to computer forensics, which allow proposing a support scheme for the attention of incidents that compromise the computer security of companies.

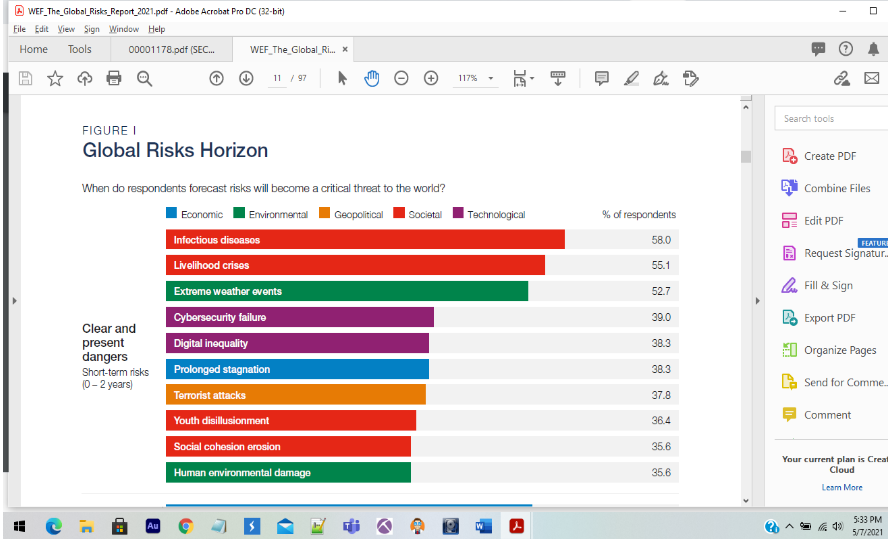
Through the reading of digital documents such as thesis works, journals, articles and publications, retrieved from information repositories such as ScienceDirect, Scopus, ProQuest, Springer, Wiley Online Library, SciELO, Directory Of Open Access Journals - DOAJ and Redalyc, managed to identify and acquire the knowledge and inputs to propose a methodology to support the technology infrastructure in terms of digital security, with a focus on the generation of traces that serve as support to the forensic investigator in the processes of identification and collection of digital evidence, For which, multiple sources of information have been analyzed, providing added value to business processes related to technology management.

Methodology

With the profound change in social, economic, and political dynamics, derived from the global pandemic declared on March 11, 2020, by the WHO (World Health Organization), PAHO (2020) technology took an even greater role from that moment, business, social networks, education, commerce and many more, saw the need to increase their presence in digital media, accelerating and increasing digital migration around the world.

Recognizing this trend, the World Economic Forum, in its sixteenth edition of the Global Risk Report 2021, M. Mclennan (2021), collects the opinions and concerns expressed by leaders around the world, where it is clear that the technological aspect , specifically that related to cybersecurity flaws is among the first critical threats with 39% agreement among those surveyed (Figure 1), because infrastructures and corporate cybersecurity measures are often exceeded by multiple attacks each increasingly sophisticated, or become obsolete by increasingly automated and frequent cybercrimes, generating economic disruption, financial losses, geopolitical tensions and social instability.

Figure 1. Global risk horizon.


WEF_The_Global_Risks_Report_2021.pdf - Adobe Acrobat Pro DC (32-bit)
File Edit View Sign Window Help
Home Tools 00001178.pdf (SEC... WEF_The_Global_Ri... ×
11 / 97 117%
Search tools
Create PDF
Combine Files
Edit PDF
Request Signatur..
Fill & Sign
Export PDF
Organize Pages
Send for Comme..
Comment
Your current plan is Creat Cloud
Learn More
5:33 PM 5/7/2021
FIGURE I
Global Risks Horizon
When do respondents forecast risks will become a critical threat to the world?
Economic
Environmental
Geopolitical
Societal
Technological
% of respondents
Clear and present dangers
Short-term risks (0 – 2 years)
Infectious diseases 58.0
Livelihood crises 55.1
Extreme weather events 52.7
Cybersecurity failure 39.0
Digital inequality 38.3
Prolonged stagnation 38.3
Terrorist attacks 37.8
Youth disillusionment 36.4
Social cohesion erosion 35.6
Human environmental damage 35.6

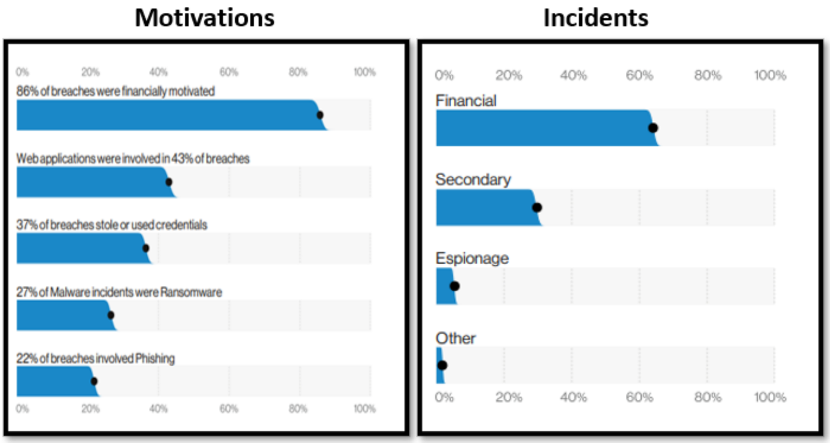
Source: World Economic Forum, 2021

In 2020, the World Economic Forum, M. McLennan (2020), noted that fraud and financial crime was a trillion-dollar industry, reporting that private companies spent approximately $ 8.2 billion just on controls against the Money laundering, all detected and undetected crimes, has become more numerous and costly than ever. In one estimate, for every dollar of fraud, institutions lose nearly three dollars, as the associated costs are added to the fraud loss itself, to efforts to correct and counteract the effects, to reputational damage., and the loss of customers, among other factors.

Specifically for financial institutions, risks arise from various factors, such as vulnerabilities to fraud and financial crime inherent in automation and digitization, massive growth in transaction volumes, as well as greater integration of financial systems of scope. National and international, for the field of monitoring and control of financial crimes, regulators continually review the rules, and governments have intensified the use of economic sanctions and regulations. Institutions are finding that their current approaches to combating such crimes cannot satisfactorily handle the many threats and burdens. For this reason, leaders are transforming their operating models to gain a holistic view of the changing landscape of financial crime. This vision becomes the starting point for efficient and effective fraud risk management. M. McLennan (2020).

The 2021 Data Breach Investigations Report published by the largest mobile phone operator in the United States Verizon Wireless, Verizon (2020), reveals an extensive and detailed work that analyzes the patterns with which breaches and incidents occur at the computer security level, I identify that in In 2020, more than four fifths of the data breaches, 86% were motivated by financial reasons, see figure 2, likewise, consistent with this trend, more than 60% of the incidents were categorized as damages that generated damages in the financial sphere.

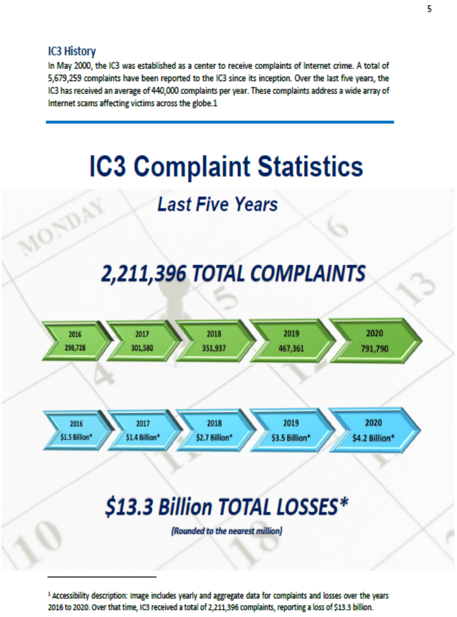
Figure 2. Motivations and incidents of cyber-attacks.



Source: Verizon, 2020

As a consequence of the use and exploitation of technology and data networks, IC3 was established as a department attached to the FBI to receive complaints about crimes on the Internet, as of the date of publication of the document, as evidenced in figure 3, it was They have reported a total of 2,211,396 complaints since the beginning of their operations, likewise, during the last five years, the IC3 has received an average of 440,000 complaints per year. These complaints address a wide range of Internet scams that affect victims around the world, it is striking that the number of complaints increased by 69.42% during 2020, compared to the immediately previous year, by far the largest increase since the start of operations of the IC3, in the same way, accumulated losses amounting to 13.3 billion dollars are recorded. P. Abbate (2021).

Figure 3. Statistics on reports received by IC3.



5

IC3 History

In May 2000, the IC3 was established as a center to receive complaints of Internet crime. A total of 5,679,259 complaints have been reported to the IC3 since its inception. Over the last five years, the IC3 has received an average of 440,000 complaints per year. These complaints address a wide array of Internet scams affecting victims across the globe.1

IC3 Complaint Statistics

Last Five Years

2,211,396 TOTAL COMPLAINTS

2016	2017	2018	2019	2020
298,728	301,580	351,937	467,361	791,790
$1.5 Billion*	$1.4 Billion*	$2.7 Billion*	$3.5 Billion*	$4.2 Billion*

$13.3 Billion TOTAL LOSSES*

(Rounded to the nearest million)

[1] Accessibility description: Image includes yearly and aggregate data for complaints and losses over the years 2016 to 2020. Over that time, IC3 received a total of 2,211,396 complaints, reporting a loss of $13.3 billion.

Source: IC3, 2021

The world-renowned expert in cybersecurity and emerging technologies Chuck Brooks (2021) reveals disturbing data regarding cybersecurity trends for this year, showing that the increase and sophistication of tools such as autonomous learning , artificial intelligence and 5G technology, facilitate cooperation between cyber attackers and in turn, the required knowledge is less and less, it also relates shocking figures, in relation to the increase in malware of 358% in 2020 and the identification of 2,145,013 Phishing sites as of January 17, 2021, which if continued without prompt attention and action, will cost the world around $ 10.5 trillion annually projected by 2025.

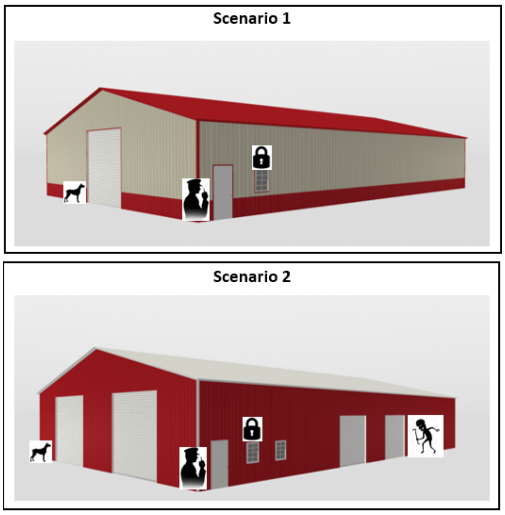
Physical security vs computer security

To better understand the importance, as well as the urgent need for the implementation of greater protection and prevention measures with a focus on computer security and the protection of technological assets, also to demonstrate that on many occasions the approach that companies take on this This topic is wrong, a simple exercise will be developed, which will show that any decision on the configuration, implementation or deployment of technological platforms generates security gaps that in many cases can go unnoticed, generating scenarios that facilitate the materialization of cyberattacks or incidents. Commonly, managers consider that a systems engineer dominates all branches of computing and is competent to solve any problem or requirement at a technological level that may arise, however, in recent decades, this branch of knowledge has grown exponential, so much so that it is stated that branches such as application development, databases and computer security, just to mention a few, are so broad that each can be considered as universes or specialties.

In the physical world there are also different specialties, for example, if you need to design a house, you turn to an architect, to build it to construction professionals, to build a road to a civil engineer, if you need to protect and protect these infrastructures, professionals in private surveillance are used, likewise, a systems engineer, in the virtual world, can specialize in design, software design, application development, server administration, design and maintenance of data networks, information storage or computer security.

Now it is proposed to carry out the same exercise specifically for the physical security of a company and then its digital equivalent (Computer Security), for which it is invited to see Figure 4, which illustrates a series of entrances to a building, including different mechanisms of access control at each point.

Figure 4. Hypothetical physical security scenarios



Source: Author

In scenario 1, a building is exemplified totally protected by all its accesses, using different protection mechanisms, which involve people, animals, and objectives, these measures require dedication, verification, and rules to react to certain situations that may arise. In theory, any access to the facilities should be controlled; In scenario 2, it is evidenced that there are multiple entries, some with protection and others totally neglected, a situation that facilitates the conditions for a security breach to be generated and access to the facilities, anyone who observes the second scenario, I would intuitively express that this protection scheme does not make sense, since the attackers would avoid protected accesses and enter through unprotected places, rendering any measure useless.

However, in many technological infrastructures, unfortunately scenario 2 occurs more frequently than would be expected, platforms are constantly being developed and deployed that generate gaps and security failures and are not protected, understanding that although there are different ways configuration and security, no platform is inherently secure, this feature must be provided, developed and strengthened in conjunction with configuration parameters, policies and access controls, in essence, as well as hiring a professional in private security for physical facilities , the same precautions must also be taken for the technological infrastructure.

Security measures such as agents, cameras, biometric devices, among others, are not used only to react to possible situations of violation, that is, they are not only there to determine which people can or cannot enter, although it is one of its main functions, they are also responsible for taking the data of the person who enters, that is, a traceability is generated, who? Who is looking for? When? Where? Is it authorized? In short, they also provide a subsequent control and verification, to identify responsibilities and those involved when an event has already occurred and it is subsequently detected; It is this traceability that, as we will see later, begins to play a determining role in favor of the forensic investigator.

As a rule, the more dynamic and open an application, service, website, or platform is, the greater the degree of exposure and provocation generated among cybercriminals, for this reason, the greater the control and registration requirements, in addition It turns out that the attacker can not only enter the virtual facilities of the companies, but he can also commit multiple crimes.

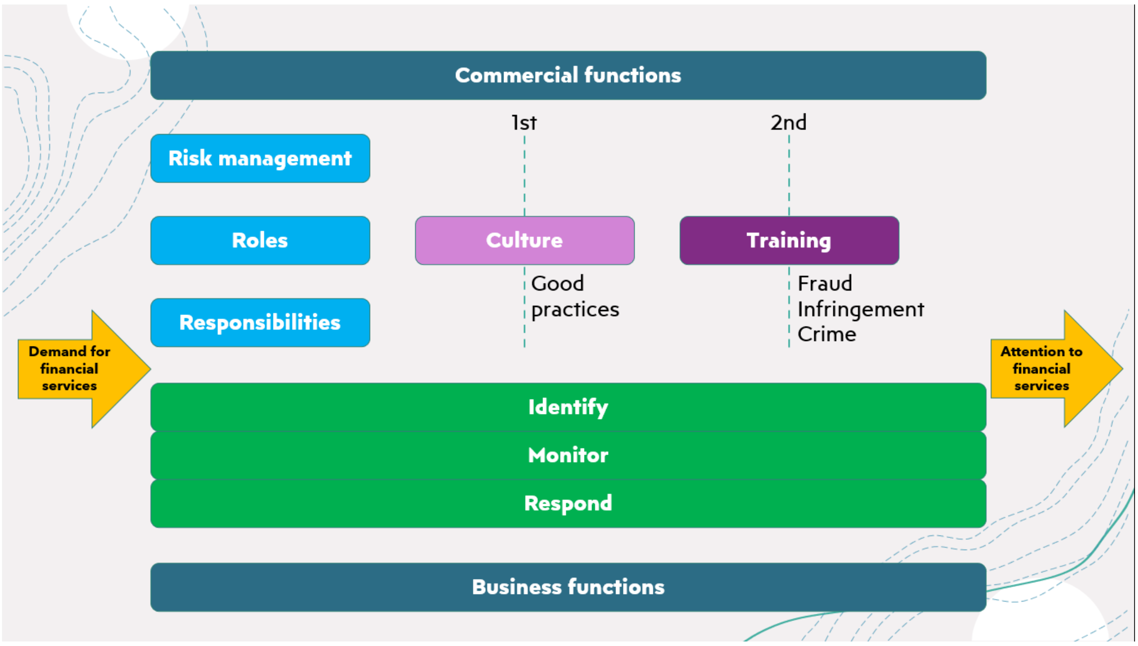
A large percentage of financial institutions have not yet addressed these issues in a holistic way, risks that go beyond what can be called the border lines that have traditionally been erected with a focus on attacking and counteracting certain types of crimes, leaving aside strengthening the generation According to money magazine, digital evidence of an incident after it occurred, can take up to 7 months after a company discovers that it has suffered a breach at the computer security level. Money Magazine (2021). As banks begin to align their operations with the changing profile of financial crime, increasingly deep connections are being identified between cyber breaches and most types of financial crime, the cyber component is not new. Since until not long, most of the fraud was developed around transactions, and criminals took advantage of weaknesses in the controls they had, financial institutions try to counteract this type of fraud with controls based on specific points communication channels, which are generally relatively straightforward, but with the rise in technology for commerce, largely due to the COVID pandemic, identity-based fraud has become more prevalent as scammers develop applications to scan services and capture data, making cyber-attacks increasingly popular. ambitious and ubiquitous.

Results

Taking into account these postulates and concerns, a methodology based on the organization of functions is proposed, which allows generating at all times the greatest amount of traces on the operation and interaction between systems and people, under this scheme, and starting from the postulate that No system is totally reliable and safe, the fact that a security incident will eventually materialize is assumed, it will be possible to accumulate the largest amount of digital evidence that will serve as support before a forensic digital investigation space.

It is necessary to join forces in matters of financial crimes, fraud, and computer crimes. The methodology begins with the demand for financial services by clients or homologous entities, including robust mechanisms of control, verification, and registration, to consider as completed with the attention to this initial demand, as can be seen in figure 5 with the boxes indicated in yellow.

Figure 5. Methodology for the generation of supports that support the collection of digital evidence



Source: Author

Both customer-facing operations, commercial functions, and back-office (business functions), outlined in dark blue in figure 5, should be oriented towards combating cybercrime, but also facilitating the forensic investigation process, It is necessary to clarify that it is not only a regulatory issue, but it is considered to be on the near horizon of attention, the important initial steps for institutions that embark on an integration effort are to define precisely the nature of all activities related to risk management and clarify the roles and responsibilities in the lines of defense (see figure 5, light blue color). These steps will ensure complete and clearly delineated coverage, by business and business functions (first line of defense) and by risk, including financial crime, fraud, and cyber operations (second line of defense), (Purple in Figure 5) when time that duplication of effort is eliminated.

The first line of defense is associated with the generation of an adequate business culture in terms of computer security implemented by the bank with all its employees and collaborators, it is expected that because of good practices and implementation of security policies, the processes have initial protection.

The second line is of a more technical nature, since it involves the attention by personnel with a higher degree of training and knowledge associated with the identification of possible fraud, infractions, and crimes, for this line, it is also necessary to have a deep knowledge of the internal processes and how they are managed by the bank, to be able to recognize irregular behavior and anomalies in the attention to financial services.

All risks associated with financial crime involve three types of countermeasures:

Identify and authenticate the customer,
Monitor and detect transactions and behavioral anomalies,
Respond to mitigate risks and problems.

As has been known for many years, it is not possible to create a 100% secure and invulnerable system, so the focus shifted from designing apparently inviolable systems to systems that quickly evidence behaviors, patterns, and anomalies, that is, to focus on the detection of incidents in the field. as little time as possible, to have a quick reaction, which allows mitigating and counteracting damages and losses.

In this same sense, the advancement and development of Forensic Informatics that began in the 1980s, has shown that the approach must evolve from the mere collection, systematization and recording of evidences that may be identified, to the planning a scheme that allows the maximum generation of traces (records remain in the log, in databases, on servers, in Web applications, email servers) and although clearly some can be falsified, when rebuilding an event through multiple servers with different roles, it will be possible to collect and validate the evidence, in other words, actions that facilitate the traceability of all the processes carried out by means of technological tools.

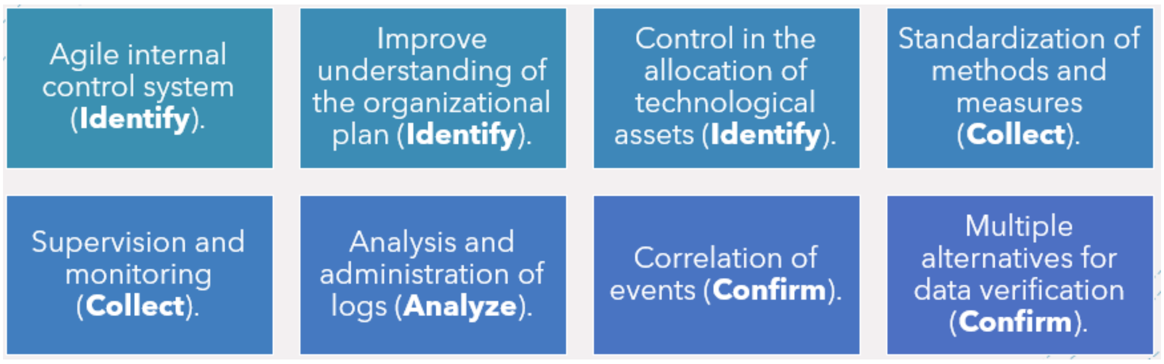
With the proposed model, each of these activities, whether carried out in response to fraud, breaches, cybersecurity attacks or other financial crimes, will be supported by many similar data and processes. In fact, combining these data sources with analytics substantially improves visibility while providing much deeper insight to increase detection capabilities.

Analysis and discussion

Computer forensics is based on four fundamental pillars: identify, collect, analyze, and confirm, unlike computer security, forensic investigators not only focus on preventing, but in the event of an incident, they seek to obtain the greatest amount of possible evidence, in the proposed scheme, highly reliable evidence is generated before a forensic investigation process and an eventual legal process.

It is expected that through the methodology for the generation of supports that support the collection of digital evidence, based on the organization of business functions proposed in this article, the processes of identification, collection, analysis, and confirmation that are so necessary will be strengthened. For the development of investigations on financial crimes that have increasingly higher rates of occurrence, such aspects are indicated in figure 6.

Figure 6. Aspects for the management of digital forensic investigation


Agile internal control system (**Identify**).
Improve understanding of the organizational plan (**Identify**).
Control in the allocation of technological assets (**Identify**).
Standardization of methods and measures (**Collect**).
Supervision and monitoring (**Collect**).
Analysis and administration of logs (**Analyze**).
Correlation of events (**Confirm**).
Multiple alternatives for data verification (**Confirm**).

Source: Author

Agile internal control system (Identify).
It is achieved with the support of internal and external audit exercises, which, developed objectively, allows to improve the operations of organizations, speeding up access to information, this aspect also provides a systematic approach in the evaluation and increase of effectiveness of risk management, infrastructure control and governance processes.

Improve understanding of the organizational plan (Identify).
When the collaborators know and apply the processes, the information is normalized, facilitating the recognition of possible sources of digital evidence, in the same way, it will be easier to detect anomalies such as attempts to alter records or anti-forensic techniques.

Control in the allocation of technological assets (Identify).
When there is control, tools are provided to optimize the search for evidence, as well as the recognition of the possible actions taken during a security incident, it will also be possible to generate greater sources and supports for the evidence.

Standardization of methods and measures (Collect).
Once the sources of evidence have been identified, the researcher must proceed to collect these, when the standards are in place and are applied, a greater degree of coherence is provided to the information collected and its respective sources, that is, a greater degree of coherence. reliability and quality of data.

Supervision and monitoring (Collect).
This aspect allows immediate interventions or in less time, likewise, it is possible to mitigate the manipulation, alteration and / or elimination of evidence, researchers can include within their supports, elements derived from these processes, such as reports, minutes, and other documents of support.

Apart from this moment, the work is carried out at the laboratory level, where actions such as Analysis and administration of logs (Analyze), Correlation of events (Confirm) and multiple alternatives for data verification (Confirm) will be developed.

Conclusions

As more aspects of everyday life are transferred to the virtual world, an increase in the number, incidence and scope of cybercrimes is evident, for this reason, sectors such as finance must adopt a more holistic vision, in relation to the scheme protection of all the main and underlying processes, hoping not only to strengthen its computer protection mechanisms, but also, a surveillance scheme should be thought about that facilitates the identification of an incident in the shortest possible time, to achieve the shortest time response; In order to also take advantage of all the lessons learned from a cyber-attack, it is necessary to collect as much information as possible, which is possible under the proposed scheme, as it invites us to optimize business processes.

Clearly, the regulations and legislation related to the classification of cybercrimes must also be strengthened, this scenario is only possible to develop in conjunction with the state and its representatives, who can take international standards such as SOX or PCI DSS Payment Card as a starting point. Industry Data Security Standard, the first, regulates financial accounting and auditing functions, designing mechanisms to counteract financial fraud, the second, proposes procedures and policies to improve security in payment by electronic means made by customers.

The more and better standards are applied within the commercial and business processes, the easier it will be to monitor and control the attention of financial services, making it difficult to create scenarios that can be exploited by cybercriminals, such as vulnerabilities, malware applications, phishing, among others, because in most cases, attackers take advantage of these spaces or gaps at the business architecture level and at the legal level.

References

Abbate, P. (2021). 2020 INTERNET CRIME REPORT. https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf

Almanza, R. (2019). XIX Encuesta Nacional de Seguridad Informática, Sistemas, vol. 151, no. 0120–5919, p. 88. https://sistemas.acis.org.co/index.php/sistemas/issue/view/4/1

Alkhanafseh, M., M. Qatawneh, & W. Almobaideen. (2019). A Survey of Various Frameworks and Solutions in all Branches of Digital Forensics with a Focus on Cloud Forensics," Int. J. Adv. Comput. Sci. Appl., vol. 10, 2019, doi: 10.14569/IJACSA.2019.0100880 Available: https://www.researchgate.net/publication/335694535_A_Survey_of_Various_Frameworks_and_Solutions_in_all_Branches_of_Digital_Forensics_with_a_Focus_on_Cloud_Forensics

Arburola, A. (2014). Auditoría forense, Monografias. https://www.monografias.com/trabajos65/auditoria-forense/auditoria-forense

Caicedo, S. & Higuera, A. (2019). Estrategias de prevención y detección del fraude financiero en las empresas de la Ciudadela Parque Industrial de Duitama. https://repositorio.uptc.edu.co/handle/001/3111.

Ceballos, L., García, F. B., Guzman, L. M. & Quintero, C. A. (2019). Tendencias Cibercrimen Colombia 2019-2020. https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf

Chuck Brooks. (marzo 2021). "Alarming Cybersecurity Stats: What You Need to Know For 2021." https://www.forbes.com/sites/chuckbrooks/2021/03/02/alarming-cybersecurity-stats-------what-you-need-to-know-for-2021/?sh=538f8a0358d3.

Fernandez, E. & R. de J. G. Herrera. (2020). Prevención de riesgos por ciberseguridad desde la auditoria forense: conjugando el talento humano organizacional, NOVUM, 10(1), p. 80. https://revistas.unal.edu.co/index.php/novum/article/view/84210/73652

Graeme, H. (2020). Part 1: - quality assurance mechanisms for digital forensic investigations: Introducing the Verification of Digital Evidence (VODE) framework. Forensic Sci. Int. Reports, vol. 2, p. 100038. DOI: https://doi.org/10.1016/j.fsir.2019.100038

Gorham, M. (2020). 2019 Internet Crime Report. https://pdf.ic3.gov/2019_IC3Report.pdf

Hall, M. (2020). Burning Planet: Climate Fires and Political Flame Wars Rage. https://www.weforum.org/press/2020/01/burning-planet-climate-fires-and-political-flame-wars-rage/

Kebande, V. (2018). A Novel Cloud Forensic Readiness Service Model | Request PDF. https://www.researchgate.net/publication/331980982_A_Novel_Cloud_Forensic_Readiness_Service_Model

López Reina, L.D., J. C. Rincón Leal. (2019), Mecanismos de recolección de pruebas forenses en los encargos de aseguramiento contable aplicables al sector cooperativo de ahorro y crédito. https://oai:repository.ucc.edu.co:20.500.12494/13694

M. & McLennan. (2020). The Global Risks Report 2020 Insight Report 15th Edition. http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf

M. M. & M. A. Pang Albert. (2019). Top 10 ERP Software Vendors, Market Size and Market Forecast 2018-2023, Apps Run World. https://www.appsruntheworld.com/top-10-erp-software-vendors-and-market-forecast/

Mclennan, M. (2021). The Global Risks Report 2021 16th Edition Strategic Partners. http://wef.ch/risks2021

Mora, D. & Ramírez, L. (2019). Delitos informáticos contables en Villavicencio. Universidad Cooperativa de Colombia, Facultad de Ciencias Económicas, Administrativas y Contables, Contaduría Pública, Villavicencio. https://repository.ucc.edu.co/handle/20.500.12494/12018

Obando, A. M. (2019). Informática forense desde el recurso humano y tecnológico, en las instituciones judiciales que cuentan con el servicio especializado de peritaje informático en Colombia. Universidad Externado de Colombia, 16, p. 122. https://bdigital.uexternado.edu.co/handle/001/1696

OPS. (2020). La OMS caracteriza a COVID-19 como una pandemia - OPS/OMS, Organización Panamericana de la Salud. https://www.paho.org/es/noticias/11-3-2020-oms-caracteriza-covid-19-como-pandemia

Pena, D. A. G. (2018). Procesos de informática forense y marco legal colombiano. Inform. FORENSE, vol. 11, p. 48. http://repository.unipiloto.edu.co/handle/20.500.12277/2736

Restrepo, L. & A. Rodríguez. (2019). La contribución de la auditoría forense en la disminución de fraudes financieros en Colombia. Tecnológico de Antioquia, Medellín. https://ojs.tdea.edu.co/index.php/agora/article/view/735

Revista Dinero, (2020). Una empresa puede tardar hasta 7 meses en detectar un ataque cibernético. https://www.dinero.com/tecnologia/articulo/cuanto-tiempo-tarda-una-empresa-en-detectar-un-ataque-cibernetico/299701

S. De, M. S. Barik, and I. Banerjee, "A Digital Forensic Process Model for Cloud Computing," in 2020 IEEE Calcutta Conference, CALCON 2020 - Proceedings, Feb. 2020, pp. 106–110, DOI: https://ieeexplore.ieee.org/document/9106500

S. Verma, S. S. Bhattacharyya, and S. Kumar, "An extension of the technology acceptance model in the big data analytics system implementation environment," Inf. Process. Manag., vol. 54, no. 5, pp. 791–806, 2018, DOI: https://doi.org/10.1016/j.ipm.2018.01.004

Verizon. (2019). Data breach investigations report. Verizon RISK Team. https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf

erizon. (2020). DBRI 2021 Data Breach Investigations Report. https://enterprise.verizon.com/resources/reports/2021-data-breach-investigations-report.pdf

X. Lin. (2018). Introductory Computer Forensics, Springer I. Springer International Publishing. https://www.springer.com/gp/book/9783030005801