UNIVERSIDAD DISTRITAL
FRANCISCO JOSÉ DE CALDAS

Visión Electrónica

https://revistas.udistrital.edu.co/index.php/visele

VISIÓN ELECTRÓNICA

A CASE-STUDY VISION

Integration and Interoperability of Electronic Health Records

Integración e Interoperabilidad de la Historia Clínica Electrónica

Lilia Edith Aparicio Pico [1], *William Barragan Zaque* [2]

INFORMACIÓN DEL ARTÍCULO

Historia del artículo:
Enviado: 27/02/2024
Recibido: 11/03/2024
Aceptado: 22/05/2024

Keywords:
Health Records
Information Security
Infrastructure
Interoperability
Platform
User Subjectivity

CC BY NC

Palabras clave:
Historia clínica
Seguridad de la Información
Infraestructura
Interoperabilidad
Plataforma
Subjetividad de los Usuarios

ABSTRACT

This article presents the fieldwork conducted in hospitals in Bogotá with the intention of finding the elements that make clinical history information vulnerable, considering the subjectivity of users about information security aspects. The study is conducted as part of the field investigation to set up a security architecture for the management of information in clinical records.

RESUMEN

El presente artículo muestra los resultados del trabajo de campo realizado en hospitales de Bogotá, con el objeto de establecer los elementos que hacen vulnerable la información en la historia clínica teniendo en cuenta la subjetividad de los usuarios en cuanto a los aspectos de seguridad de información. El trabajo se desarrolla como parte de la investigación de campo para establecer una arquitectura de seguridad para la gestión de información en Historias Clínicas.

1 Licenciada en Ciencias de la Educación - Física, Universidad Distrital Francisco José de Caldas, Colombia. Magister en Teleinformática, Universidad Distrital Francisco José de Caldas, Colombia y Doctor en Ciencias Técnicas, Universidad Central "Marta Abreu" de las Villas, Cuba. Current position: Director del grupo Gitem++, Profesor Titular / Universidad Distrital Francisco José de Caldas, Colombia. E-mail: medicina@udistrital.edu.co

2 Ingeniero Catastral y Geodesia, Universidad Distrital Francisco José de Caldas, Colombia. Especialista SIG, Universidad Distrital Francisco José de Caldas, Colombia, Magister en Fotogrametría, Univerisad de Ciencias Aplicadas de Stuttgart, Alemania y Doctor en Educación, Universidad de California, Estados Unidos. Current position: Miembro del grupo Gitem++, Profesor Titular, Universidad Distrital Francisco José de Caldas, Colombia. E-mail: wbarraganz@udistrital.edu.co

Citar este artículo como: L. E. Aparicio, W. Barragan "Integration and Interoperability of Electronic Health Records", Visión electrónica, vol. 17, no. 1, pp. 131-145 January-June 2024, https://doi.org/10.14483/22484728.23379

1. Introduction

This article presents the results of a Security Architecture for Clinical History Management project. As another outcome of the research, a diagnosis of the study, access, and usage behavior of Clinical Histories in Bogotá hospitals are provided. This case study served as the basis for analyzing the requirements of a security infrastructure for managing such information.

In another instance, there is an exploration of basic clinical history management processes, revealing that most hospitals use heterogeneous and fragmented systems. Therefore, the integration of a single Electronic Clinical History (ECH) becomes a priority.

Consequently, it becomes necessary to define interoperability as 'the ability of ICT systems and supporting processes to exchange data and share information and knowledge.

It is essential to gain a clear understanding of the current state of existing systems and the behavior of healthcare organizations. The fact that existing infrastructures were necessary in the past, aligned with the technology of their time, does not justify their replacement with entirely new systems. Consequently, healthcare entities should implement or fully keep operational those system that their professionals find most useful for their practice. Considering that 'ICT applications across the entire spectrum of healthcare functions can become complex due to human responsibility and usage behavior, from the perspective of a heterogeneous distributed system under the ubiquitous system model, it is necessary to create a distributed unique system that allows for the application of legislation across its entire spectrum as outlined in Chapter 12, and in line with the knowledge base described in Chapter 2.

This deduction arises because it is challenging to speak of a single centralized system, even though it is clear and accepted that the ECH must be unique and a core element of the e-Health infrastructure. This is a transitional period from a network of isolated systems to one of connected and interoperable systems. It is now possible to find different sets of information related to citizens' health data that need to be unified before taking part in a global project. In fact, this unification must begin with some urgency and priority. Thus, goals for different projects can be found, such as achieving a unique ECH within a hospital, with various usage scopes but of multiple uses and subject to the relevant security restrictions. This implies having a clear aim of achieving a unique ECH for health area or an Autonomous Community, simply by unifying all the earlier ones into a single system.

Solutions to this situation share many common factors. It has been acknowledged by working groups in the international eHealth forum that it is not possible to think of a single architecture to address the challenges posed by different health information systems converging in the management of clinical history and their multiple aims. They conclude that the solution to sharing information and functionality in a coordinated manner requires the availability of an 'interoperability environment' that integrates solutions and highly restricted access information.

Consequently, the proposal for a security architecture for electronic clinical history information management gains certainty as access, security, usage, and current regulatory issues are resolved. This is achieved through the interconnection of logical systems built on integration platforms and a new generation of 'connectable applications.

2. Methodology

Once the current state of use, processes, and procedures of the Clinical History [1] had been found, it was analyzed that it is necessary to find aspects of vulnerability in the information based on the usage

patterns of the different users within the healthcare system in Bogotá. To carry out this, reference work on security architecture platforms was consulted, and their possibilities were analyzed to infer the use of technology in real environments. In this regard, the stages of the vulnerability method for this work were as follows:

2.1 Critical Analysis of Needs in the Security Model for Clinical History Management

It can be concluded that there are several characteristics of the current clinical history system. Additionally, common characteristics of the applications supporting the operation of local area networks in organizations were considered. Based on a study conducted in the Capital District in 2009, the following conclusions can be drawn:

- Independence of centralized entities.
- There should be ease of use without obstructing the user. Ease of use and non-interruption to the user are essential requirements for a ubiquitous environment. A user-friendly system is more secure than a complex one [2]. Users should not be interrupted in their task to provide the system with any information, and processes should be automated as much as possible to avoid distractions [3; 4].
- Support for disconnections is necessary. Users of the system are mobile and will enter and exit constantly. Support for disconnections is crucial.
- Interoperability: There is incompatibility among the systems supporting the applications. In such cases, programs must be changed or built from scratch to use the mechanisms of the new environment. In some systems, these modifications can be extremely costly [5].
- Simplicity: Traceability of the system should be eased, and the system should be highly adaptable [6].
- Extensibility: the possibility of adding new devices to the system should be provided, in line with the development of other applications, such as Telemedicine.

To implement a new application, it will no longer be necessary to dismantle what already exists. Instead, only what is truly obsolete should be replaced without affecting the rest. Applications should be developed to be connectable within this interoperability environment. This is where difficulties related to legal (security, privacy, consent), operational (flow, process, documentation, supervision), exchange (coding standards, documentation, semantics), and technical (accessibility, uniqueness, availability, performance, scalability) components must be resolved. The integration infrastructure supporting interoperability, in addition to accommodating modern integration standards, must also address integration with non-standard environments that need to be kept for a medium-term transition, primarily for cost-saving reasons. The fact that there are many applications in full operation that do not support new standards does not justify their elimination and replacement with others that perform the same functions. An interoperability environment must provide all its participating members with the full set of recognized standards, both semantic and technological, along with tools that allow those who do not have such standards to take part.

2.2 Strategic Advantages

From the perspective of computer security, an effective security architecture allows an organization to develop or keep its strategic and competitive advantages, Information, technology, and personnel are critical resources distributed throughout the organization and form the basis or its operational infrastructure. The rapid development and adoption of

new technologies and their expansion within organizations have supplied competitive advantages, increased productivity, and exposure to new markets. However, this rapid expansion has also created new risk for which management has limited experience and, in some instances, has inhibited expansion into those unknown markets. To remain competitive, companies must be prepared to expand their zones of trust. To properly consider the increased risk, management needs to address control and security of critical resources with an enterprise-wide approach.

In recent years, various tools have been set up to have intrusion detectors to check and assess Internet security within the organization. Being on the information highway is no longer a luxury but a necessity in today's economy. However, many businesses have integrated new technologies and capabilities with little or no awareness of security. Furthermore, many businesses have bought security-related technologies and have not properly installed, integrated or kept them, leaving them vulnerable in their technological security infrastructure.

For years, companies have hired external consultants to provide comparisons with other businesses about security and technology operations. As part of these services, consultants supplied action plans to implement corrective measures. In most cases, these action plans were filed away and never implemented. To be effective, security must be constantly adaptive. Today's solution is tomorrow's risk. Many organizations do not have the ability to dedicate resources to staying updated and aware of constant changes in technology and strategy. Now more than ever, there is a reliance on external resources to provide solutions to organizations, offering the talent and ability to ensure that technology and strategy are suitable and integrated with the strategic and tactical needs of the business. However, the electronic medical records system is complex and requires special treatment.

Security today is more than passwords, firewalls, and audit trails. It also involves training personnel to understand not only the technologies in place but also their integration and impact on business operations. To achieve this, organizations need reliable advisors to find shortcomings and weaknesses, design system and process improvements, and integrate effective solutions. CTG's Computer Security Solutions offer practical solutions that meet client needs. Through our security assessment software tools, and management knowledge portals, we supply consistent recommendations and proactive responses to mitigate risks.

Over the last 30 years, computing has fundamentally changed from high centralization in an environment of large data centers, which is easy to control, to the current virtual environment where controls, if they exist, are constantly changing, leading to modern platforms in distributed environments such as those needed for electronic clinical history management.

2.3 Analysis of User Behavior

Behavioral analysis about users of different types (e.g., doctors, patients, the community) and different systems and programs used for clinical history management was conducted. This analysis was aimed at understanding the information usage patterns of the organization.

From a technological standpoint, it is advisable to analyze the following characteristics that differentiate centralized and distributed environments to find elements of conflict that need to be resolved.

In a centralized environment:

- Access is restricted to a limited number of users.
- Processes are primarily batch-based, often with extended periods between activities.

- There are redundant manual controls.
- Data is centrally archived with minimal volume.
- The introduction of personal computers in 1978 marked the beginning of the democratization of computing, moving processing from controlled areas to general workspaces.

In the distributed environment:

- There is a growing number of users, but all stay known and authorized by the organization.
- Processing frequency jumps from daily to hourly or on demand.
- Network environments allow multiple distributed users in a physical location.
- Taking computers out of controlled areas has increased the diversity and success of portable technology.
- When the influence of information technology expands to all operational, financial, human resources, and sale functions, the need for a common language in programs becomes a high priority for achieving efficiency.

It can be concluded that there are several characteristics of the current clinical history system. Additionally, common characteristics of the applications supporting the operation of local area networks in organizations were considered Based on a study conducted in the Capital District in 2009, the following conclusions can be drawn:

- Independence od's Centralized Entities
- There must be ease of use and no obstruction to the user. Ease of use and non-interruption to the user are essential requirements for a ubiquitous environment. A user-friendly system is more secure than a complex one [2]. The user should not have to interrupt their tasks to provide the system with any type of information, and processes should be automated to the greatest extent possible to avoid distraction [3; 4].
- Support for Disconnections: It is necessary to support disconnections and delegation. System users are mobile and will constantly enter and exit the system. Since the system should be as user-friendly as possible, and user exits from the environment are unpredictable, disconnections need to be supporting the applications. In such cases, programs must be changed or built from scratch to use the mechanisms of the pristine environment. In some systems, these modifications can be extremely costly [5].
- Simplicity: The traceability of the system should be eased, and the system should be highly adaptable [6].
- Extensibility: The possibility of including new devices in the system should be provided, in line with the development of other applications, such as Telemedicine.

To implement a new application, it will no longer be necessary to dismantle what already exists. Instead, only what is genuinely obsolete should be replaced without affecting the rest. This will be achieved by developing applications that can connect within this interoperability environment. This is where difficulties related to legal components (security, privacy, consent); operational components (flow, process, document, supervision); exchange components (accessibility, uniqueness, availability, performance, scalability) must be resolved. The integration infrastructure that will support interoperability, in addition to accommodating modern integration standards, must also resolve integration with existing non-standard environments that need to be kept for a medium-term transition, primarily to save costs. The reality that there are many fully operational

applications that do not support new standards does not sufficiently justify their elimination and replacement with others that perform the same functions. An interoperability environment must offer all participating members the complete set of recognized standards, both semantic and technological, along with tools that enable the participation of those who do not have such standards.

With the advent of the Internet/Intranet/Extranets, which have enabled the virtual environment and high-speed networks:

- Every parameter that existed previously has been redefined.
- Updates are constant.
- The computerized environment is now global.
- Storage technology allows for unlimited ability. Organizations no longer have full knowledge of who is connected to their systems at any given moment, and control points change rapidly.
- To connect with others, protocols and standards are being reconsidered.

From a business perspective, in line with the evolution of technology, there has been a significant shift in the level of risk within organizations. Risks run in two realms:

- One is the realm of business, with trends and a focus on cost reduction, rapid changes, increasing complexity, and short-term results.
- The other is the risk that arises from the technological environment as it evolves into an open environment with more users, connection points, complexity, and reduced reaction time.

Today, the level of risk has not been replaced but has indeed expanded over time. Earlier risks persist in the current world and grow exponentially with new risks appearing from modern technology.

Finally, it is essential to implement security policies, among which it can be considered that computer system security primarily focuses on ensuring the right to access data and system resources by configuring authentication and control mechanisms that ensure users of these resources only have the rights granted to them.

2.4 Designing a Survey Based on the Hypothesis of High Information Risk Due to User Subjectivity

However, security mechanisms can sometimes cause inconveniences for users. Frequently, instructions and rules become increasingly complex as the network grows. Therefore, computer security must be studied in a way that does not hinder users from developing necessary uses and safely using information systems.

For this reason, one of the first steps a company must take is to define a security policy that can be implemented based on the following four stages:

1. Finding the security needs and computer risks facing the company, along with their potential consequences.
2. Supplying an overview of the rules and procedures to be implemented in response to found risks across different departments of the organization.
3. Monitoring and detecting vulnerabilities in the information system and staying informed about deficiencies in applications and materials used.
4. Defining actions to take and individuals to contact if finding a threat.

The security policy encompasses all the rules an organization follows concerning security (in the general sense of the word). Consequently, the organization's management should handle defining it since it affects all system users. Some causes of insecurity can be considered as follows.

Insecurity can be divided into two categories:

5. An active state of insecurity, meaning the user lacks knowledge about the system's functions, some of which can be detrimental to the system (e.g., not deactivating network services not needed by the user).
6. A passive state of insecurity, meaning the user or system administrator lacks knowledge of available security measures (e.g., when they are unaware of the security devices at their disposal).

2.5 Survey Context

To set up the requirements of the proposal from a unique perspective, a survey was conducted to find and find the vulnerable points in the control of information handled by users of the current medical history system. From this perspective, a current context of information and knowledge about the security platform had by the healthcare entities under study was presented.

This is a present viewpoint, and what we aim to present is a modern approach from distributed environments. This clarification is important to mention what the knowledge context was for conducting the survey from the point view of the current system. Additionally, to motivate the survey, a historical analysis of information security, not of networks, was performed, which is outlined below.

Security is a basic need, encompassing aspects such as the prevention of loss of life and possessions. [7]

The earliest concepts of security can be traced back to the beginnings of writing with the Sumerians (3000 BC) or Hammurabi (2000 BC). The Bible, homer, Cicero and Caesar have also authored works where certain elements of security in warfare and government are clear. [8]

Archaeological discoveries undoubtedly mark the most considerable evidence of security in ancient times, including the Egyptian pyramids, the palace of Sargon, the Karnak temple in the Nile Valley, and the Egyptian god Anubis depicted with a key in hand, among others.

Like any concept, security has evolved and followed a developmental path within a social organization. Society initially formed around family units, which became a limiting factor for escape. New strategies of intimidation and deterrence had to be conceived to convince attackers that the losses were unacceptable compared to potential gains.

The first evidence of a "mature" security culture and organization appears in the documents of the Public Networks (state) of the Imperial and Republican Rome. The next step in security was specialization. This gave rise to External Security (concerned with threats from external entities to the organization) and Internal Security (concerned with threats within the organization itself). From these two categories, Private Security and Public Security appeared when the state entrusted its trust to armed units.

Since the 18th century, scientific discoveries and the resulting knowledge form printing have contributed to the culture of security. The principles of probability, prediction, and failure and loss reduction have shed new light on security systems. [9]

Modern security originated with the Industrial Revolution to combat crimes and labor movements. Finally, a management theorist and pioneer, Henry Fayol, in 1919, found Security as one of the business functions, following technical, commercial, financial, accounting, and managerial functions. [10]

In the current era of communication and networks, security is primarily focused on information security, which is in the hands of organizational management, each of the system users, and all active and passive members of a communication system, where the user

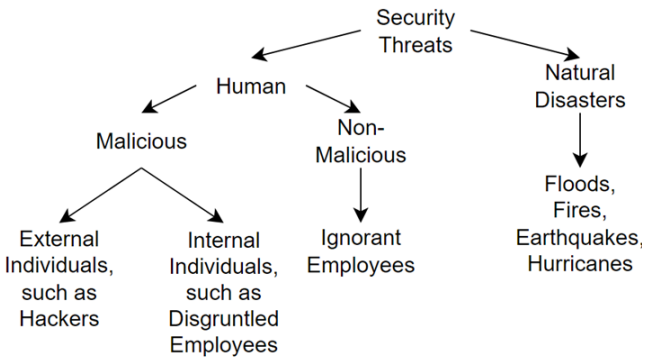
can be seen as the primary element that introduces vulnerability.

Currently, there is no strict definition of what is understood by information security, as it encompasses multiple and diverse areas related to Information Systems, ranging from the physical protection of the computer as hardware components and its environment to the protection of the information it has or the networks that connect it to the outside.

Regarding data, which is the smallest unit that composes certain information that conveys meaning [10], it is essential to preserve their integrity, availability, operability, privacy or confidentiality, control, authenticity. Additionally, protection against replication and non-repudiation must be ensured, which requires safeguarding the hardware and software to protect them from factors considered as anything that can expose the system to vulnerability and attack.

From the user's perspective, threats or situations that compromise the system can be classified as shown in Figure 1, where natural threats endanger the physical components of the system, human threats, which require special care because they depend on knowledge, responsibility, and awareness of the importance of information for an organization, and malicious threats expose hacker attacks, based on which security policies are designed.

Figure 1. Security Threats. [12]



Among the several types of attacks [12], [13], [14], passive attacks are included, where the attacker does not disrupt the communication but merely listens to or checks it to obtain transmitted information. Their aims are data interception and traffic analysis. Active attacks, such as interruption, interception, modification, fabrication, destruction, and added attacks like error exploitation attacks, monitoring attacks, "Shoulder Surfing" or physical espionage, authentication attacks, and denial attacks, highlight the need to employ vulnerability identification techniques from the user's perspective. This is the primary focus of this article in developing a strategy that enables any organization to work on security policies based on the types of users within their organization. [15]

Table 1. Security Regulations.

	Year 2017 %	Year 2018 %	Percentage Diffetence
1 to 10	90,3	90,6	0,3
11 to 20	3,9	6,6	**2,7**
21 to 50	3,9	1,9	2
More than 50	0	0,9	0,9
None	1,9	0	1,9

	Year 2019 %	Year 2020 %
None	26,8	26
1 to 5	58,2	58
6 to 10	10,9	5
11 to 15	0,9	5
More than 15	3,2	6

Source: own.

In terms of regulatory compliance, Table 1 illustrates the behavior about control provisions for small and medium-sized enterprises, which recognize the importance of information security as an added value and a significant business strategy to build trust among their clients in the use of their technological infrastructures. While this position is optimistic, it is not universal due to the investments needed to achieve

elevated levels of security and control in their computing architectures.

The security approach focusing on user vulnerability underscores the importance of addressing threats as the primary measure for information security. Table 2 presents the threat between the years 2017 and 2020.

The data considers the first five years of web page and portal exploitation. As of the present date, the sample size has increased but still is unchanged, reflecting common user behavior as seen in the diagnostic. [1]

Table 2. Threats in Information Security.

Threats	Year 2017 %	Year 2018 %	Year 2019 %	Year 2020 %
None	5,4	8,7	6,6	9
Software Application Manipulation	4,5	4,3	5,8	8
Unauthorized Web Access	14,8	10,6	9,4	10
Fraud	4	3,9	1,8	5
Viruses	33,6	33,3	34,9	29
Data Theft	3,6	3,9	2,6	2
Trojans (Trojan Horses)	4,9	4,8	10,0	11
Unauthorized Traffic Monitoring	4,9	7,7	5,8	8
Denial of Service	6,3	7,2	7,6	7
Loss of Integrity	6,7	3,9	2,9	3
Loss of Information	9,4	10,1	10,5	7
Other, please specify – attempts, if they occurred were not detected, channel congestion.	1,8	1,4	2,1	1

Source: own.

It is confirmed that viruses are the most frequent source of computer security failures. Similarly, the modification of website pages, internal employee abuses, and denial of service are highlighted as the most recurring in this region of the world.

In other aspects, the lack of executive support and technological complexity appear as prominent trends in this section of the survey. Information security, like business strategies, requires a process of rationalization and marketing, and having support organizations eases protection efforts. Table 3 shows the access behavior to support organizations in recent years.

Table 3. External Support Organizations.

Support Organizations	Year 2017 %	Year 2018 %	Year 2019 %	Year 2020 %
Yes, please specify which ones: DAS, Prosecutor's Office, SIJIN, FBI, Incocrédito, internal company organization.	13,5	11,7	7,4	61
No	72,1	66	66,4	30
Do not know	14,4	22,3	26,2	9

Source: own.

It is noted that organizations are seeking support from law enforcement agencies to carry out and complete their investigations. Likewise, the mechanisms provided by the government to address security incidents or intrusions, such as the cybercrime units of the DAS and SIJIN, are being given and publicized. However, this cannot be the exclusive effort of these units but must be supported by a national-level strategy that channels and enhances the efforts of academia, government, organizations, and industry.

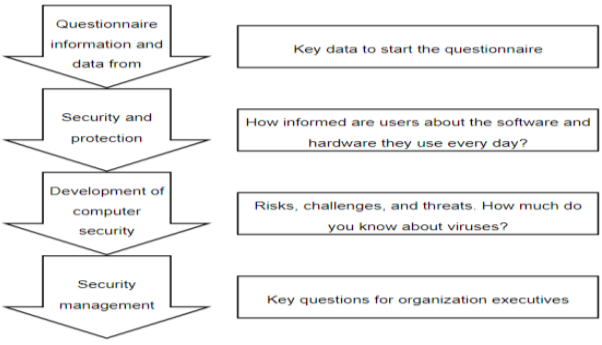
Exploratory research was conducted, and 7 HEALTHCARE ENTITIES were selected as primary sources for obtaining basic information. Information was gathered from specialized books on computer security, viruses, hackers, technical standards for research work, dictionaries, and encyclopedias, all of which supplied extensive information on vulnerabilities, threats, and risks faces by information systems. The most consulted source was the Internet,

as it encompasses comprehensive knowledge of security topics from around the world.

The primary data collection instrument was a survey conducted through questionnaires. These questionnaires applied to issues that could be investigated through observation, analysis of documentary sources, and other knowledge systems. The standardization parameters of the questionnaire included: Aim of the questionnaire, which aimed to obtain information about feelings and knowledge of Computer Security for the improvement of security strategies within the organization. Variables in the questionnaire included Hardware, Software, Vulnerabilities, Threats, and security policies, infrastructure.

Survey Guide: The survey is divided into five (5) chapters that cover various aspects, subdividing the use level to find vulnerability aspects, as shown in Figure 2.

Figure 2. Survey Application Model.



Source: own.

The information processing was carried out by tabulating and organizing the data, which were subjected to statistical techniques, and the results are reflected based on them.

The survey targeted the following user groups: the organization's executives, mid-level management employees with basic knowledge of systems, and employees from the IT department.

To gather the information, we approached individuals who had the relevant information, considering the aspects shown in Table 4:

Table 4. Relevant Population Aspects.

Relevant Aspects	Actividad
Gender	Man or woman.
Age	Over 18 years old
Activity	Managers, Directors, Analysts, Assistants, Office Clerks, Engineers, Technologists, Students, and Professionals
Education	Professionals, any activity
Profession	Any profession
Specific characteristics	Who needs to use a PC and use it in their work activity?

Source: own.

The sample was random with a size of 282, with a margin of error of 0.055, belonging to an approximate population of 356 individuals who are in both the systems and administrative areas, in both the private and public sectors.

3. Discussion

Among the main results inferred form the collected data are the following:

- Only 12% of organizations are confident in their ability to detect a system attack.
- 73% of users do not investigate or analyze incidents related to their systems.
- Critical business systems often experience disruptions, with approximately 82% of organizations reporting unexpected system unavailability due to computer viruses.

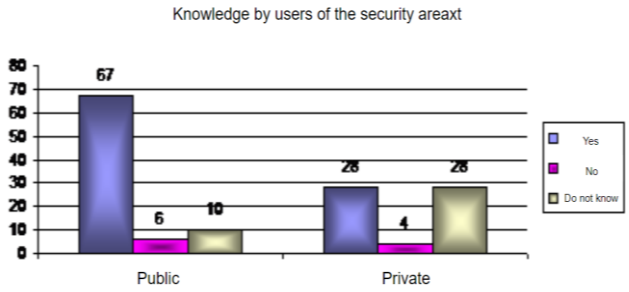
- 73% of organizations have protection against hardware and software theft.
- Less than 50% of organizations have computer security awareness programs in place.
- The most used computer security technologies today are access control (passwords), antivirus software, and firewalls.
- 83% of organizational leaders do not know how much they are spending on information security or where exactly those expenditures are going.

Regarding control data on security, information security is often still considered primarily a technical issue, typically handled by the Information Systems department. This translates into a focus on implementing only the technical aspects, technological solutions that do not support business processes, and point solutions such as firewalls or antivirus protection.

The greatest danger lies in senior management believing that their company is adequately protected when substantial technical investments are underutilized due to inadequate business processes, lack of awareness or training, third parties or partners, and a lack of security measure reviews to assess their effectiveness.

Of the organizations surveyed, 66% have a formal Information Security department. I n public entities, employees are aware of the department's existence, while in the private sector, half of the employees are aware, and the other half have no knowledge of its existence. Figure 3 presents the results of this analysis.

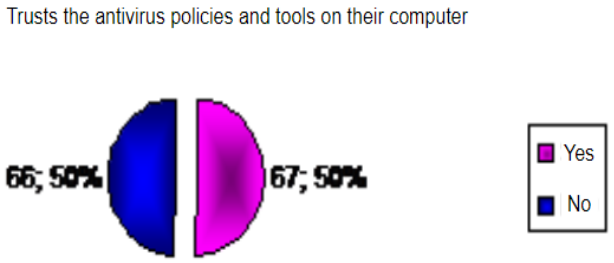
Figure 3. Knowledge of the Security Area.



Source: own.

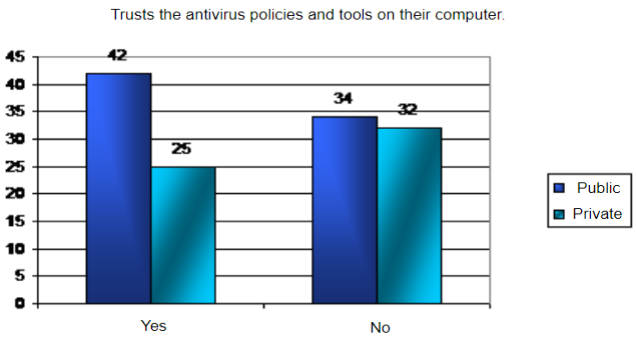
According to the data obtained, the trust in security policies and virus protection tolls coincided with the results, as 50% trust and 50% do not trust these policies. However, when looking at the results by sector, public organizations have greater trust un these policies and tools compared to private organizations. Figures 4 and 5 illustrate this situation.

Figure 4. Trust in Security Policies.



Source: own.

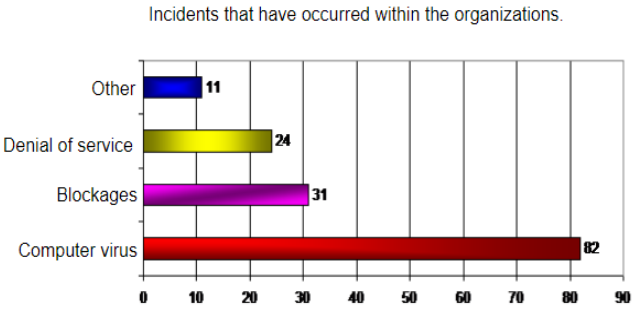
Figure 5. Trust in Security Policies



Source: own.

Security Policies by Sector. 66% of the respondents mention that there is a barrier to achieving effective security, but still less than half of the companies have training in security and employee awareness programs. Regarding incidents, the most frequent causes of interruptions are due to software and hardware failures (31%) and telecommunications failures due to viruses (82%). A quarter of the failures were due to operational errors, lack of system ability, or third-party failures. Figure 6 has the results of incidents reported within organizations.

Figure 6. Incidents Reported Within Organizations.



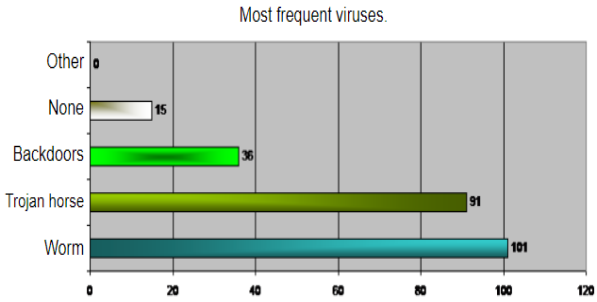
Source: own.

The respondents consider the impact of failures on operations as equally important as their impact on financials or reputation. More than half of the respondents have business continuity plans. However, among those with plans, only 37% have conducted a business impact analysis and prioritized their critical processes, and 73% have not tested the plan. Additionally, less than half of the respondents have managed to agree on critical recovery times, suggesting a gap between what the business needs and what the continuity plan can provide.

A higher number of organizations claim to have system disaster recovery plans (71%), but 16% have not tested them. Management may question whether it is worth recovering hardware and software if the staff does not have a place or procedures to continue critical business activities. Regarding incidents, the most common ones were viruses like Worm and Trojan Horse, which caused irreversible damage to the system.

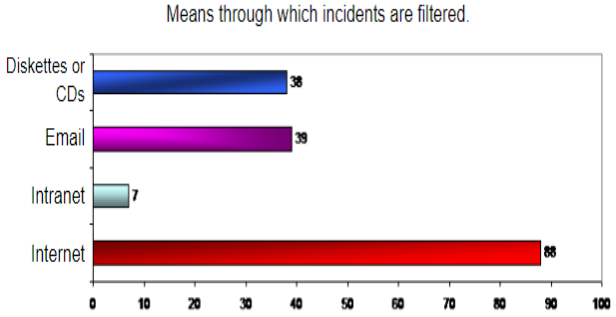
The most frequent viruses are listened to in Figure 7, and Figure 8 shows a breakdown of the most common means through which incidents manifest.

Figure 7. Most Common Viruses.



Source: own.

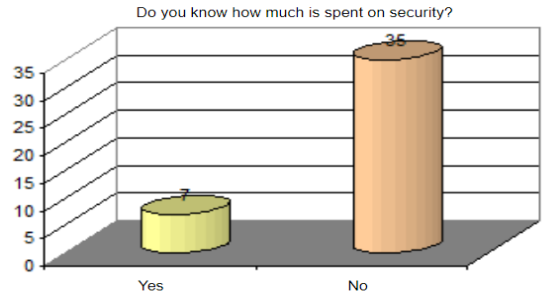
Figure 8. Most Common Virus Transmission Methods.



Source: own.

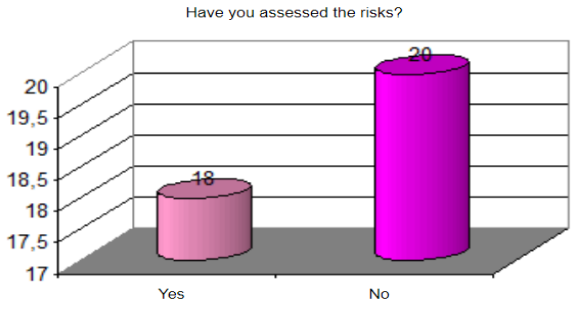
Regarding technology and access controls, it was found that access control (passwords), antivirus software, and firewalls were the most used, followed by encryption of files and virtual private networks (VPNs) in a secondary position. Another important aspect is security management, with Figures 9 and 10 highlighting aspects of executive awareness about investment in information security, yielding the following results.

Figure 9. Risk Assessment.



Source: own.

Figure 10. Security Cost.



Source: own.

Investment in information security may appear in the overall IT budget or in the budget of each business unit. However, it is most concerning that 53% of the organizations have not assessed the costs associated with the risks that could result from a cyberattack.

Other general findings include:

- 73% of the respondents do not investigate security incidents, although this deficiency increases the likelihood of not detecting damage or the creation of "backdoors" for later unauthorized use.
- Only 40% of the respondents admitted to having suffered an attack on their data networks or Internet serves. This is unusual when compared to other statistics showing a higher likelihood of attacks. However, it is known that many companies do not openly admit to having been targeted by cyberattacks.
- Additionally, only 12% of the respondents are confident in their ability to detect an attack. It seems probable that some of those who trust in their ability to detect an attack have been attacked but are unaware of it.

4. Conclusions

To achieve the overall aims, a study was conducted using the application of theory and basic security concepts, along with research techniques. This study aimed to understand the level of security and protection kept by the organizations that took part in the fieldwork. The collected information was coded and tabulated to obtain counts, classifications, and organization in tables and charts.

The main conclusions are as follows:

- Many organizations are grappling with frequent interruptions of their critical systems, uninvestigated security incidents, a lack of business continuity plan, limited employee awareness, and the challenge posed by the increasing sophistication of threats.
- The most used information security technologies today are access control (passwords), antivirus software, and firewalls.
- 83% of organizational executives do not know how much they are spending on information security and precisely where those expenditures are going.
- Only 12% of the respondents are confident in their ability to detect an attack. It is likely that some of those who trust un their ability

to detect an attack have been targeted, but they are unaware of it.

Based on the survey results, the necessary insights have been obtained to consider architecture centered on users rather than platforms, which will be the focus of the final research proposal.

A security architecture should be proposed that addresses the needs of information security while also accommodating innovations in technological environments characteristic of distributed technologies, as analyzed in earlier chapters.

In summary, from a pragmatic point of view, as proved in the fieldwork, there are unresolved aspects, such as:

- Clinical and health information, concepts, functions, and characteristics.
- Individual identification.
- Single and shared health records, records for each center and isolated records for each center that are accessible from other centers; health records for each center and health records with information originating from all healthcare centers.
- How clinical information is organized or structured, including information architecture.
- Integration of departmental information: laboratories, pharmacies, diagnostic imaging, and other clinical administrative systems.
- Integration of information from systems complementary to clinical systems, such as occupational health, public health, and complementary services.
- Genetic and genomic information.
- Information standards.
- Application of legal provisions related to medical records to electronic medical records.
- Information security and confidentiality.
- Inferences from the clinical information system.
- Electronic medical records and their implications for research and education.

References

[1] L. E. Aparicio, "*Informe Diagnóstico del estado actual de uso de las historias clínicas en hospitales de Bogotá,"* 2010.

[2] B. Schneier, "*Beyond Fear: Thinking Sensibly about Security in an Uncertain World,"* Copernicus Books, New York, NY, 2003.

[3] R. Campbell, J. Al-Muhtadi, P. Naldurg, G. Sampemane, y M. Mickunas, "Towards Security of Privacy for Pervasive Computing," en *Proceedings of the International Symposium on Software Security, LNCS 2603*, pp. 1–15, Springer-Verlag, 2002.

[4] D. Garlan, D. Siewiprek, A. Smailagic, y P. Steenkiste, "Project AURA: Toward Distraction-Free Pervasive Computing," *IEEE Pervasive Computing*, vol. 1, no. 2, pp. 22–31, 2002.

[5] M. Ulrich, "*Legacy Systems: Transformation Strategies*," Prentice Hall PTR, 2002.

[6] J. H. Saltzer, D. P. Reed, y D. D. Clark, "End-to-End Arguments in System Design," *ACM Transactions on Computer Systems*, vol. 2, no. 4, pp. 277–288, 1984.

[7] G. Manuta, "*Presentación del libro 'Seguridad: una Introducción',"* Revista de Seguridad Corporativa, [Online]. Available: http://www.seguridadcorporativa.org

[8] C. F. Borghello, "*Seguridad Informática: Sus implicaciones e implementación*," Tesis, [Online]. junio 2001. [Citado: nov. 5, 2004]. Available: http://www.segu-info.com.ar/

[9] R. P. Fisher, "*Seguridad en los temas informáticos*," Madrid, p. 85, 1998.

[10] J. A. Jiménez, "*Evolución Seguridad de un Sistema de Información,"* [Online]. nov. 2001, Available: http://www.Monografías.com/trabajos/introc/introc.sthml

[11] R. F. Calvo, "*Glosario básico inglés-español para usuario,"* [Online]. feb. 2000, Available: http://ati.es/novatita/2000/i45

[12] J. C. Ardita, "*Entrevista personal,"* Cybsec S.A., [Online]. ene. 15, 2001, Available: http://www.cybsec.com

[13] M. Merlat, G. Paz, M. Sosa, y M. Martínez, "*Seguridad Informática: Hackers,"* [Online]. jul. 2003, Available: http://www.SeguridadInformáticaHackerilustrados com.htm

[14] K. J. Jones, Superutilidades Hackers, México D.F.: McGraw Hill, 2003, pp. 282–288.

[15] F. J. Suñer, "*Hacker,"* [Online]. jul. 2004, Available: http://www.ciencia-ficcion.com/glosario/hacker.htm

[16] J. Cano, "V Encuesta Nacional sobre Seguridad Informática en Colombia," [Online]. ene. 2005, Available: http://www.acis.org.co/index.php?id=452

[17] C. E. Méndez, *Metodología Diseño y Desarrollo del Proceso de Investigación*, Bogotá: McGraw Hill, 2005.