RDBCI | Revista Digital de Biblioteconomia e Ciência da Informação
Digital Journal of Library and Information Science

ISSN 1678-765X doi 10.20396/rdbci.v19i00.8665529

ARTICLE

Information and communications security management
ergonomic assessment to evaluate unsafe behaviors

Rogério Batista dos Santos [1] https://orcid.org/0000-0001-8545-4236
Tiago Barros Pontes e Silva [2] https://orcid.org/0000-0003-2149-5973

[1] Brazilian Agricultural Research Company, Brasília, DF, Brazil / e-mail: rogerio.bst@gmail.com
[2] University of Brasília, Brasília, DF, Brazil / e-mail: tiagobps@gmail.com

ABSTRACT
Introduction: This report consists of a case study on the unsafe behavior of employees of a Federal Public Administration Institution from the Ergonomics perspective. Thus, from the understanding of the concepts of Information Security and the Ergonomic Approach, we seek to identify the main factors that lead the subject to assume behaviors that put the institution's Information Security at risk when performing their daily work activities. Methods: The data were collected through observations of the work in real conditions, considering its variability, the work situation and the instruments used to carry out daily activities. Interviews were also carried out in the work context to assist the researchers in understanding the employees' behaviors. Results: There were identified cases in which the difficulty in following the institution's safety recommendations is related to a conflict existing in the work organization itself. Conclusion: The present study points to an issue that requires further study in the literature: the conflict in the work prescription itself. This may be one of the factors responsible for the difficulty of people in behaving safely in Brazilian public institutions

KEYWORDS
User behavior. Ergonomics. Information security.

Gestão da segurança da informação e comunicações
análise ergonômica para avaliação de comportamentos inseguros

RESUMO
Introdução: Este relato consiste em um estudo de caso sobre o comportamento inseguro dos funcionários de uma Instituição da Administração Pública Federal sob a ótica da Ergonomia. Assim, a partir da compreensão dos conceitos da Segurança da Informação e da Abordagem Ergonômica, busca-se identificar os principais fatores que levam o sujeito a assumir comportamentos que colocam em risco a Segurança da Informação da instituição ao desempenhar suas atividades cotidianas do trabalho. Método: Os dados foram coletados por meio de observações do trabalho em condições reais, levando em consideração a sua variabilidade, a situação de trabalho e os instrumentos utilizados para a realização das atividades cotidianas. Também foram realizadas entrevistas no contexto de trabalho para auxiliar os pesquisadores na compreensão dos comportamentos dos funcionários. Resultados: Foram identificados casos em que a dificuldade em seguir as recomendações de segurança da instituição está relacionada a um conflito existente na própria organização do trabalho. Conclusão: O presente trabalho aponta para uma questão que demanda maior aprofundamento na literatura: o conflito existente na própria prescrição de trabalho. Esse pode ser um dos fatores responsáveis pela dificuldade das pessoas em se comportarem de maneira segura nas instituições púbicas brasileiras.

PALAVRAS-CHAVE
Comportamento do usuário. Ergonomia. Segurança da informação.

JITA: BJ. Communication

1 INTRODUCTION

Nowadays, technological advances have significantly changed the way we produce, organize, and make information available. The increase in communication capacity, the interaction between systems, the evolution of convergent networks, and the emergence of mobile networks have been providing continuous communication in several places, enabling several ways to access information. Initially, these environments were designed for research purposes, aiming to allow several connectivity possibilities between the interacting parties and, therefore, security was not in focus in their initial conception. Today, with the growth of commercial demand and the strategic use of communications through these means, Information Security (IS) has become a priority factor for corporations that need to keep their information secure, such as the launch of a new product on the market, or the credit card numbers of their customers.

For private companies and public organizations, the effective use of information and communications with the help of Information Technology (IT) enables them to increase the efficiency of their operations. Data about customers, products, services, and the business circulate through the various sectors of the corporate environment, helping operational employees and managers to carry out their daily activities. The influence of Information Systems on the performance of organizations can be seen in all operational and managerial areas of companies. Such systems aim to collect, retrieve, process, store and distribute information, automatically or not, involving in their process people, machines, and organized methods. Organizations have become increasingly dependent on the availability of these systems for the maintenance of their workflow. To ensure that information is accessible when required, protected from unauthorized access, and in integrity, Information Security implements a series of security controls such as policies, procedures, practices, organizational structures, hardware, and software.

The benefits of deploying, managing, and controlling IS in organizations go beyond the initially intended privacy characteristics and add properties that help organizations reach their goals (FRÓIO, 2008). For Balloni (2007), Information Systems Security must contemplate not only the technical aspects but also the social aspects, related to the organizational environment and the people. Fontes, Balloni, and Laudon (2015, p. 2) further state that "we must consider the culture of the organization and its moment of participation in the market". Therefore, in addition to considering all the physical factors, such as environments and equipment, people must also be considered.

It is necessary to pay attention to maintaining the physical, psychological, and social integrity of the human being in the work context, avoiding that the adversities of the current times weaken this, which is the determining factor of Safety. In this scenario, we can see that competitiveness, productivity, and the search for information protection, among other factors, have made organizations adopt several technological tools and management methodologies to achieve their goals. However, these pre-established compositions do not always provide complete and sufficient solutions to be directly applied, for not contemplating the aspects of people's contextualized action as being significant for the result of the work.

Thus, guided by the Ergonomic perspective, we seek to explore the activities performed by people within an organization, to understand why the prescriptions (policies, standards, and rules) have not been fulfilled as expected. Supported by methods and techniques of own analysis, the ergonomic action seeks answers to problems resulting from the inadequacy of artifacts, work for an organization, and environments to the human way of functioning (ABRAHÃO et al., 2009). With it, the real work of the subject is investigated, respecting its

variability, as well as the work situation and the instruments.

In the daily work of institutions connected to the Brazilian Government, incidents related to Information Security are common. The Federal Public Administration Institution (IAPF) in which the research was conducted, not identified due to information protection issues, is an example in which these adversities have directly impacted its normal workflow. Common examples of insecure behavior that can be observed in the institution are password sharing, sharing information with permissions beyond those required, the use of technological equipment of a private nature within the institution, among others. Thus, the need arises to understand the factors that lead people to adopt this behavior.

Therefore, the objective of this work is to identify the main factors related to unsafe behaviors adopted in the Federal Public Institution. For this purpose, it is intended to: describe the Information Security guidelines and recommendations in force in the institution at the time the research was conducted; describe the main Information Security incidents that occurred in the IAPF in the period; identify the employees' behaviors related to the incidents considered unsafe, and report the difficulties of people in complying with the security guidelines.

It is noteworthy that the exact year of data collection will also be omitted in the report for institutional protection purposes. However, the evolution of the current regulations on the subject is observed, such as, for example, the Institution of the National Information Security Policy (PNSI), formalized by Decree No. 9,637 of December 2018 (BRASIL, 2018). In the same sense, it is important to consider that the data collection occurred before the COVID-19 pandemic that began in 2020, so that all the implications of the use of technologies for remote work, and their consequences in terms of information security, were not contemplated in the present study.

2 INFORMATION SECURITY

In the past, the issue of Information Security was much simpler, data was stored on paper in drawers and files. Security consisted only in restricting physical access to that location. With the arrival of large computers, the security structure became more sophisticated, with logical access controls, physical security of the computing environment, and awareness of the few people involved. With the advent of personal computers, mobile devices, and converged networks, the security aspects have become complex. Data and information are continuously being accessed from multiple locations, the possibilities for use are wider than with closed systems, and so are the risks to privacy and information integrity.

The increasing use of Information Technology (IT) for various personal activities, such as leisure and work, is a central feature of the information society. Although a portion of the data and information available in Information Systems is intended for public access, other operations require some level of security, such as transactions with credit card numbers, bank account data, and access to private information. In this sense, Cybersecurity is defined by

> actions aimed at the security of operations, in order to ensure that information systems are able to withstand events in cyberspace capable of compromising the availability, integrity, confidentiality, and authenticity of stored, processed, or transmitted data and of the services that these systems offer or make accessible. (BRAZIL, 2019).

In a broader perspective, for the American psychologist Abraham Maslow (1954), security is basic stability desired by everyone. It is a human need that arises to the extent that physiological needs are reasonably satisfied, such as; eating, sleeping, and breathing. "Only human beings and their organizations are capable of developing or achieving security". (FERNANDES, 2009, p. 9).

Before discussing security in the informational context, it is necessary to define the concept of information. Information is the result of processing existing data about someone or something, a set of facts organized in such a way that they acquire additional value beyond the value of the fact itself (STAIR, 1998). It consists of "data, processed or not, that can be used for the production and transmission of knowledge, contained in any medium, support or format" (BRASIL, 2019). When intact and available, it has highly significant value and can represent great power for those who possess it, as it allows its holders to take initiatives or even anticipate action, produce knowledge and apply it to their needs, and to new demands originated in the enrichment of life, whether personal or organizational.

Information is the attribution of meaning to a set of data. Data can be understood as a sequence of symbols and is a syntactic entity. It is just an index, a record, an objective manifestation, amenable to analysis, requiring a person's interpretation for its manipulation. Data can be represented by sounds, images, texts, numbers, and structures, and when these are organized or configured in a meaningful way, they become information (SIMON, 1999).

For companies, the ability to capture and absorb information correctly and agilely determines their possibilities of innovating products, increasing profitability and serving their customers well, being competitive in a highly unstable and agile market such as the present times. According to Chiavegatto (2002), the lack of appropriate information and knowledge as a subsidy to the decision-making process causes slowness, inefficiency, and increased costs when implementing actions. Given this, organizations feel the need to make use of information, proactively and dynamically, to ensure survival in an increasingly complex and competitive environment.

The economic role of information as an input for product development, fundraising, market knowledge, and survival of many companies in the private sector becomes clearer every day. As far as the public sector is concerned, the use of information and knowledge is not aimed at market competitiveness, but rather at the provision of services for the benefit of society in a given locality. In public organizations, Information Security (IS) is used to increase the possibility of providing good services to citizens. Whether public or private, the purpose of an organization concerning IS is always the same: to protect the organization's most important resources, whether tangible or not, such as physical resources, financial resources, its legal position, institutional knowledge, etc.

In this sense, Information Security can be understood by "actions that aim to enable and ensure the availability, integrity, confidentiality and authenticity of information" (BRASIL, 2019). Tampered information, not available when needed, under the domain of people of bad faith or competitors, can expose the organization and its professionals to considerable losses.

Every day the Information Systems and computer networks of organizations are tested by various types of threats. For Dias (2000), information is a company's main asset and is under constant risk

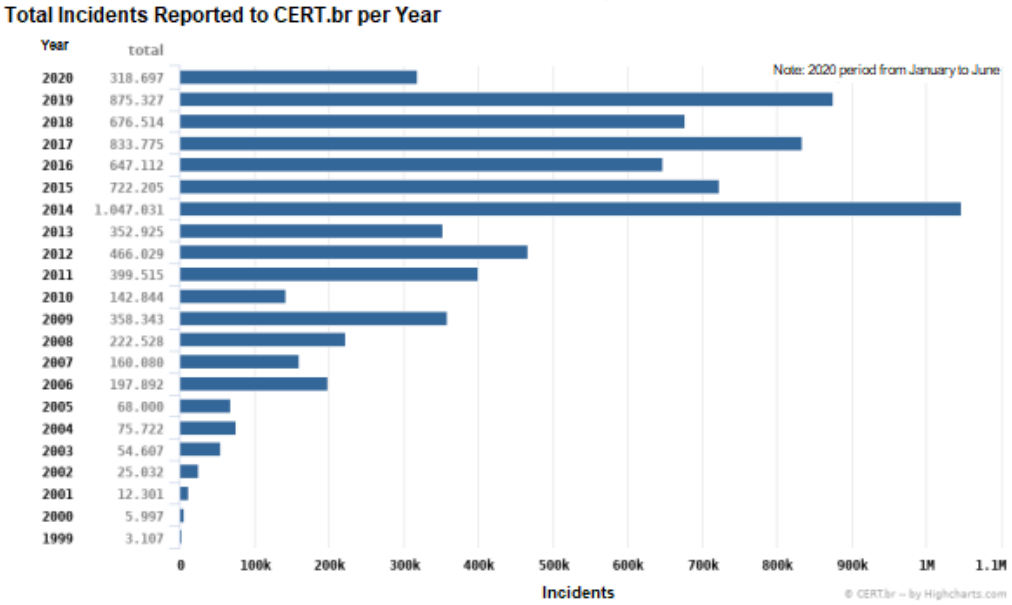
> Cada vez mais as organizações, seus sistemas de informação e redes de computadores são colocados à prova por diversos tipos de ameaças à SIC, incluindo fraudes eletrônicas, roubo de informação, espionagem, sabotagem, vandalismo, fogo, inundação e outros acidentes. (NETTO, FREIRE e ALEMMAND, 2008, p. 6).

Given this fact, the information must be adequately protected, as well as the environments and equipment used for the processing, which are also under constant threat.

Problems caused by viruses, hackers, and system unavailability are becoming increasingly common, more ambitious, and more sophisticated (ABNT, 2005). According to the Center for Studies, Response, and Treatment of Security Incidents in Brazil (CERT.br), the

total number of reported incidents has been growing considerably in recent years, reaching 875,327 cases in 2019 (Figure 1).

Figure 1. Statistics of Incidents Reported to CERT.br



Fonte: http://www.cert.br/stats/incidentes
Source: http://www.cert.br/stats/incidentes

In the current context, organizations are dependent on Information Systems, which are growing in quantity and complexity, and which control the most varied types of operations, as well as the flow of information within organizations. IS have acquired great importance for the survival of most modern organizations, not only in the image of the organization before its customers and partners but also in the progress of the organizational processes themselves. "It is possible to make the continuity of an organization unfeasible if proper attention is not given to the security of its information" (BRASIL, 2008, p 26).

In this sense, Information Security (IS) is a management process that aims to protect computational and non-computational equipment, facilities, data, and information against misuse by unauthorized third parties. This definition also encompasses equipment such as computers, faxes and photocopiers, and all types of media, even paper documents (BALLONI, 2007). The benefits of deploying, managing, and controlling information and communications in organizations go beyond simply restricting access to information. It also aims to:

a) increase user productivity through a more organized environment, providing greater control over computer resources, even enabling the use of mission-critical applications;
b) Demonstrate responsibility in favor of protecting the client and the information itself;
c) Reduce cost due to improved operational control and loss management;
d) Keeping the organization's image improved by increasing the reliability of its services;
e) Lead the company to achieve its objectives, because its information systems will be more reliable.

Therefore, it allows the organization to comply with the current legislation and codes

of ethics, maintaining its image with integrity and transparency to investors, auditors, and society. For Balloni (2007), the IS aims to ensure the availability, integrity, and confidentiality of information. Other authors also discuss the properties that must be observed to obtain secure information. According to the ABNT standard (2006), Information Security is characterized by the preservation of the availability, integrity, and confidentiality of information, besides other properties such as Authenticity, Reliability, Non-Repudiation, and Responsibility for information. For Dias (2000); Albuquerque and Ribeiro (2002) and Sêmola (2003), for information to be considered secure, the system that manages it must still respect, Authenticity, Non-repudiation, Legality, and Auditing.

Availability can be understood as the guarantee that authorized users will obtain access to the information whenever necessary and required (ALBUQUERQUE; RIBEIRO, 2002). The information stored in the Information Systems must be accessible to those entitled to it when requested. When information is prevented for some reason from being accessed when requested, the absence of availability is characterized. **Integrity** is the guarantee that information and processing methods are only altered through planned and authorized actions (NETTO, FREIRE, and ALLEMAND, 2008). Information exchanged between individuals must have the guarantee that it has not been modified. When an element, without authorization, intercepts, modifies, and forwards the message to the recipient, a breach of integrity is characterized. **Confidentiality** is the guarantee that information is accessible only to authorized people. The information exchanged between individuals and companies should not always be known by everyone, and much information generated by people is intended for a specific group of individuals, often a single person. When an unauthorized element has access to certain information and, at the same time, manipulates or stores it, a breach of confidentiality is characterized. **Authenticity** is related to the proper authorization of a particular individual or system, body, or entity that produces, sends, modifies, or destroys the organization's information. It is the identification and certainty of the information's origin. **Non-repudiation** consists in preventing an entity from participating in a given operation and later denying this participation (FRÓIO, 2008, p 12).

Also, important characteristics of the Information Security (IS) management process are **Legality**, as the guarantee that the appropriate legal measures are applied when necessary, and **Auditing**, which enables the verification and evaluation of responsibility against errors and acts committed by authorized users in information systems. To identify authors and actions, audit trails and logs are used, which record what was done in the system, by whom, and when.

Currently, Information Security is known even by company presidents, due to the importance of information in conducting business (BALLONI, 2007). According to the author, to conduct a viable business, security must ensure that the use of information in various business initiatives happens in a regulated manner.

With the dependence of the business on information systems and the emergence of new technologies and ways of working, such as e-commerce, virtual private networks, and mobile employees, companies have started to awaken to the need for security, since they have become vulnerable to a greater number of threats. This new context requires the organizations, teams, and security methods that are permanent and in constant evolution, to take into consideration the control of physical and logical access and mainly the awareness of the people involved in the process. However, this universe is subject to various forms of threats, physical or virtual, which seriously compromise the security of people and information.

A **threat** can be defined as any action, event, or entity that can act on an asset, process or person, through a vulnerability generating a certain impact. Vulnerability is a flaw in the design, implementation, configuration of a software or operating system that, when exploited by a threat, results in a security breach. When threats and **vulnerabilities** exist in a given

environment, we consequently have a security risk. **Risk** is a possible and potentially harmful event to an organism. That is a hypothetical event that has a non-zero chance of future occurrence and has a significant negative impact (FERNANDES, 2009). Any adverse events confirmed or under suspicion, that may threaten Information Security (IS) are called security **incidents**. A security **event** is the identified occurrence of a system, service, or network that indicates a possible violation of the Information Security Policy or failure of controls, or a previously unknown situation that can be relevant to Information Security (ABNT, 2005).

Besides the weaknesses internal to the Information Systems, there is the possibility of an external agent trying to obtain or modify information in an unauthorized way, such as an attack. **An attack** can be defined as an assault on the security system that derives from an intelligent threat, that is, an intelligent act that is a deliberate attempt (special in the sense of a method or technique) to break into security services and violate system policies (SHIREY, 2000). Attack is the act of trying to bypass the security controls of a system to break the aforementioned principles.

To avoid the problems related to Information Security, **controls** are used by the institution, which are all the means and devices to promote, direct, restrict, govern and verify the various activities that have as their main purpose the observation that the company's objectives are achieved. According to ABNT (2006), a series of controls must be used to conduct company business efficiently, ensuring the safeguarding of information, maintaining its availability, integrity, confidentiality, and authenticity.

Given these challenges, the need for an Information Security Management (ISM) process arises, which aims to systematize and organize the application of Information Security (IS) practices so that organizations' businesses are secure and their objectives are successfully achieved (FRÓIO, 2008).

> Information Security Management is a set of management practices and methods that aim to promote and maintain the organization's assets at acceptable and necessary levels of security so that the business objectives are achieved as planned (FRÓIO 2008, p. 14).

GSI takes a systematic approach to minimize the risk of unauthorized access or loss of information and ensuring the effective management of the protective measures in place. It provides a framework for organizations to manage their compliance with legal and other requirements, and to improve the performance of secure information management.

To compose a more complete and robust management model, Information Security Management is based on the interaction between processes, procedures, controls, best practices, and technologies to guide the models currently in use. The Information Security Policy (POSI) is a set of clearly defined rules, standards, procedures, and appropriate controls to reduce risks to acceptable levels. It contains the necessary guidelines for the safe conduct of the organization's business to ensure institutional continuity. "The adoption of policies and GSI should be a strategic decision of the organization, noting that this decision is influenced by the needs, objectives, security requirements, size and structure of the organization" (NETTO, FREIRE, and ALLEMAND, 2008, p. 4).

POSI is seen by organizations and experts as one of the most important components of a corporate security solution. It contributes to improving the behavior of the people who work in companies and manipulate information. The Information Security Policy aims to direct and support the protection of information assets against intentional or unintentional disclosure, modification, destruction or denial, through the implementation of plans that allow the immediate return of business, procedures, and routines (PELTIER, 2004). For ABNT (2005),

the purpose of the Information Security Policy is to provide guidance and support from management for Information Security following business requirements and relevant laws and regulations. Alerting to the fact that the policy document must be approved by the management, published, and communicated to all employees.

Research in Information Security reveals that in work environments, the internal problems, which involve people, are more representative than the external ones (LOPES, 2009). It is noticeable in organizations that, even after high investments in training and awareness of employees, many still tend to behave irregularly, making mistakes and carelessness that compromise Information Security. In the search for possible solutions to the process of evaluating human behavior, the optics of Ergonomics is adopted, focused on understanding the interactions between human beings and other elements or systems. Ergonomics has the analysis of the actual work situation as its main tool, guiding the ergonomic action and delimiting the most appropriate instruments and procedures for the analysis (ABRAHÃO and PINHO, 1999).

The great challenge of the ergonomic analysis in this work consists in identifying the real problems existing in the work environment of the organization regarding Information Security, which increases the risks, providing the exposure of the system vulnerabilities, resulting in losses and damages to the institution. It is believed that, from the Ergonomic perspective, focusing on the human factor, it is possible to think of policies and rules adapted to people's abilities and limitations. With this, we expect greater efficiency in the implementation and achievement of objectives in the creation of safe environments.

3 THE ERGONOMIC APPROACH

In this topic, the Ergonomics approach to investigating the behavior of people at their workstations is described. For Ergonomics, work is defined by a prescription (task) that is different from the actual work (activity). Because of these differences, people devise strategies to be able to maintain the flow of work and accomplish the goals of the task. Ergonomics aims to transform work (or even work tools) to adapt it to the characteristics and variability of people and the production process. Thus, "ergonomic action seeks answers to problems resulting from the inadequacy of artifacts, work organization and environments to the human way of functioning" (ABRAHÃO et al., 2009, p. 11).

According to the International Ergonomics Association (IEA), Ergonomics is defined as a scientific discipline related to the understanding of the interactions between humans and other elements or systems, and the application of theories, principles, data, and methods to projects in order to optimize human welfare and overall system performance (IEA, 2000). In this perspective, Ergonomics was developed adopting as reference the notion of variability, the distinction between task and activity, and the regulation of actions to the recognition of the competence of workers (ABRAHÃO et al., 2009).

The **task** can be understood as the set of prescriptions of what the worker must do according to certain norms and standards and using specific equipment and tools, according to specific standards of quality and quantity. It is not the work itself, but rather the norms, precepts, and rules that determine and authorize work. One can say that, for the worker, the task is what he has to do, with the means offered to him. **Activity**, on the other hand, is what the worker does (real), his actions, decisions, and strategies that aim to achieve the objectives defined by his task. It means what is done by the worker, the way he can develop his tasks. Thus, we can say that activity is the way people, in a real work situation, relate to the proposed goals, the work organization, the other workers, and the means provided to accomplish them.

The activity is the guiding axis for ergonomic actions; it is how the subject articulates

his/her competencies to fulfill the demands of the task, the established objective, and the effective work conditions that are given to him/her (FERREIRA, 2000). Activity is dynamic and uncertain, given the variability of people and work situations.

The **variability** in the organization of work stems from the difference between prescription and reality and can be understood considering the characteristics of the worker, emphasizing the notion of inter and intra-individual variability, and the organization of work, where the variability of the equipment and procedures is highlighted (ABRAHÃO, 2000). The human organism has limitations that influence the way we understand and act upon the world. Previous experiences modify the strategies adopted and future actions (ABRAHÃO et al., 2009). Thus, we can say that there is variability in the way each individual acts, which is an intra-individual variability. This variability is influenced by human physiological changes, such as aging, illnesses, circadian rhythm, as well as by people's formal and informal knowledge.

Therefore, it is considered that the same individual does not behave in the same way all the time. Generally, in work situations, people are not alone, and the environment is shared with other individuals. Each one has different characteristics, experiences, and doings. Thus, we can say that there is inter-individual variability. In addition to intraindividual and inter-individual variability, from the perspective of work organization, there are predictable variabilities, such as changes in the seasons, and unpredictable variabilities, such as the failure of a piece of equipment.

Work can be considered as a collective action, performed by different actors, through finalistic actions related to organizational objectives. These actions are performed under the institution's own rules and delineation, integrating the organization's culture and the workers' task-related prescriptions. Therefore, for the ergonomist, it is very important to understand the task within its organizational context. To do this, it is first necessary to understand the organization of work in each institution, its social, economic, geographic, and historical context. Only then, it is possible to situate the task in the production context in which it is inserted. Thus, each company is organized by the division of tasks, the division of people, hierarchical structures, work and break times, rhythms, and cadences.

Still, "Ergonomics can also consider cognitive and behavioral aspects in the relationship between man and work mediated by the use of artifacts, known as Cognitive Ergonomics (CE)" (ABRAHÃO et al., 2009, p 239). Its role is to make technological solutions compatible with users' characteristics and needs. CE does not aim to try to understand the nature of human cognition but to describe how human cognition affects work and is affected by it. One of the goals of analyzing cognitive processes is to understand how individuals regulate the work situation by solving problems arising from the discrepancy between what is prescribed (task) and the reality encountered.

The way the worker manages his work process can be better understood from the concept of **Action Competencies**. It can be understood as the articulation of knowledge, representations, types of reasoning, and cognitive strategies that the subject builds and modifies during the activity (MONTMOLLIN, 1990 apud ABRAHÃO et al., 2009). For Cognitive Ergonomics, the competencies are not related to the notion of excellence of performance, they are constituted by the knowledge and strategies that the individual elaborates for action. Competencies are inherent to all individuals.

The analysis and intervention adopted in the expression of human cognition take into consideration the capacities and limits of the physiological and cognitive nature of the human being. However, it is often possible to explain the origin of errors and incidents attributed to human failures. The CE is interested in understanding the reason for this "human failure" through the analysis of the processes of acquisition, processing, and retrieval of information, which constitute an important object of study (SILVINO, ABRAHÃO and SARMET, 2005).

The Competencies for Action comprise the **Representation for Action** and the Operative Strategies. According to ABRAHÃO and colleagues (2009), the Representation for Action is a cognitive structure, which can be a mental model, a mental map, an image, or even a scheme, whose function is to allow the person to understand the situation in which he/she finds him/herself and retrieve his/her knowledge to act. The knowledge used in everyday life to accomplish tasks at work are also representations. To send a fax, use a photocopier, or even make a phone call, it is necessary to evoke our knowledge, or part of it, which is most relevant according to the situation. For each different situation, different knowledge is evoked to act. It is through representations that individuals develop the most relevant strategies and the most appropriate procedures to accomplish a task.

The concept of **Operative Strategies** can be understood as an ordered set of steps involving reasoning and problem solving, enabling action (MONTMOLLIN, 1995 apud ABRAHÃO et al., 2009, p 328). Operant strategies are defined by Silvino and Abrahão (2003) as a regulatory process that presupposes cognitive mechanisms such as categorization, problem-solving, and decision-making. The Operative Strategy involves attention and problem solving that result in a set of actions called Operative Mode. The Operative Mode is a set of actions and operations that people adopt depending on the demands of the task and their competence in the work process.

In the CE, we try to understand which are the elaborated strategies that favor the directing of attention, as well as how people's attention is distributed. It is also important to identify from which elements of the situation a hierarchy is established about what is most relevant to the development of the activity. By identifying the information and strategies used in the work process in the actual situation, it is possible to define the transformation parameters or flexibility criteria to be incorporated in the process to facilitate the selection of relevant information. To respond to the demands in a diversified manner, the ergonomist needs a set of procedures and techniques with special characteristics for this range, known as Ergonomic Analysis of Work (AET).

> AET is structured in several steps that are intertwined with the objective of producing knowledge and transforming the work. We can say that it is a very open method, since the usual tools for data collection may vary and their choice is made according to the nature of the problems posed at the time of the demand (ABRAHÃO et al., 2009, p. 348).

To achieve its objectives, AET understands the interrelation man-work based on the activity, i.e., of the real situation at a micro-level of analysis that emphasizes the actions and operations of the subject, as well as their strategies to articulate their characteristics (age, skills, physical dimensions, among others) to the variability of work (production goals, equipment, environmental factors, others) (SILVINO, 2004). According to Abrahão and colleagues (2009, p. 349), "understanding work is always a challenge because it is the result of a tangle of variables that need to be apprehended in a given context." This is the common thread that guided several researchers and professionals in the ergonomic area to ceaseless research work that resulted in a method, open to complementation, useful, and validated. In this sense, it is considered pertinent to use this approach in an attempt to identify the unsafe behaviors performed in the IAPF, as well as the possible factors associated with them.

4 THE INFORMATION TECHNOLOGY IN THE IAPF STUDIED

The present report consists of a case study carried out in a public institution not identified for security reasons, called the Institution of Federal Public Administration (IAPF).

To better understand the results, the organizational structure of the IAPF and the role of its Information Technology Department in the organizational context are presented below. The Institution of Federal Public Administration (IAPF), is a public company under private law, is present in almost all the national territory with its units and some countries in Europe, Africa, and the United States. Its Headquarters is made up of Administrative Units that have the function of planning, coordinating, controlling, and evaluating the activities related to the social objectives consigned in the mission and strategies of the Company. The Administrative Units, also known as Central Units (CU's) are, along with the Executive Board, the Company's senior management bodies, which are responsible for planning, supervising, coordinating, and controlling the activities related to the institution's core business.

IT in the IAPF has the role of providing support for organizational development and maintenance of its work process. Its mission is to enable solutions in Information Technology to contribute to institutional development, sustainability, and competitiveness of the institution. The DTI acts in the development and management of corporate IT solutions for the IAPF, related to organizational and managerial aspects. There is also the Management Committee on Information Technology, which is a deliberative collegiate body that operates at the corporate level with the Executive Board, consisting of the Chief Executive Officer, heads of the main strategic processes of the Company, and heads of decentralized units.

The Information Technology Department is a technical-administrative Central Unit, responsible for the processes of providing and managing Information Technology solutions for the IAPF in order to make it more competitive. Its basic functions are to advise the Executive Board on planning and management of Information Technology and identify the needs and manage IT resources by providing innovative solutions. Strategically, the Department has the function of aligning IT with the Company's business processes and to define access policies, and manage the database and communication network environments to guarantee the security of the information that passes through or is stored there. The DTI is structured by a general head, the Information Systems, Infrastructure and User Support (AU) coordinators, and two Supervision functions.

In January 2010, AU went through a restructuring process. The former HelpDesk system is now a Service Desk, based on ITIL best practices, which is a set of best practices applied to the infrastructure, operation, and maintenance of Information Technology services. This turns the service desk into a single point of contact between users and the institution's IT service management. From this transformation, AU added new activities such as directly answering simple requests and complaints, receiving, registering, prioritizing, and following up on IT service calls, and keeping customers informed about the status and progress of their requests. Requests are made to the central office by phone, through a form on the intranet, or utilizing memos. The calls that are not the responsibility of AU are escalated (forwarded) to the other coordinations according to the attributions of each one.

The Service Center uses two types of service for employees at the IAPF headquarters. The first, through remote access, in which the attendant accesses the microcomputer of the employee who is physically distant through the local network. The second occurs in person, and the attendant must go to meet the employee. The Demands of the decentralized units, on the other hand, are answered via telephone calls. The Service Desk is the main operational interface between the IT at the IAPF headquarters and its employees, which allows the attendants to contact directly with all demands. This direct contact allows the attendant to map behaviors, collect management data and eventually identify business opportunities.

Thus, this sector is strategic to the study, because it is where all the demands related to Information Technology are registered, an essential data source to achieve the objectives of this work. The description of the DTI routine, recorded based on the previous experience of one

of the researchers as an employee of the department, is considered pertinent. According to data extracted from the DTI service order registration system, the Service Center answers a monthly average of 2,000 calls. Of these, 500 become service requests to IT. The demands that arise through memos and the form available on the intranet do not exceed 30 per month. Using the service order records provided by the DTI in the last 15 months, several problems were identified related to the behavior adopted by the IAPF employees that daily put the security of their information at risk. Examples are the sharing of passwords to access the local network and information systems, the storage of personal files (such as photos, videos, and music) on network servers. Also, the exposure of restricted access information through indiscriminate sharing and the use of flash memory and optical media can be easily stolen, lost, or damaged to store corporate files, and this situation worsens when these devices are privately owned.

In addition, personal equipment such as notebooks, netbooks, and palmtops are used to access the organization's local network, workstations are not locked during the employee's absence from the workstation, and every type of printed document has remained on the desk. Also, several users have administrative privileges on their workstations, and often programs are found installed by the employees themselves without the proper licenses or prohibited by the DTI. Likewise, employees change the default configuration of the workstations' operating system and even go as far as to remove basic programs such as the antivirus. Furthermore, employees from administrative departments are observed within the organization developing applications and small information systems without authorization. Regarding the organization's communication systems, the use of telephone extensions and VoIP is not controlled. Only electronic mail has rules for its regulation.

These insecure behaviors put IAPF's Information and Communications at risk, as they allow vulnerabilities to be exploited by internal and external threats, causing possible security incidents. Although the IAPF does not officially register the Information Security incidents, it is possible to observe some in records from other DTI information systems. Thus, in face of the problems presented, it is verified that several occurrences can happen generated by irregular behaviors related to Information Security at the IAPF Headquarters. In this sense, a more detailed description of the institution's security guidelines, as well as the unsafe behaviors of its employees, is considered pertinent.

5 METHODOLOGY

Work is part of the company's organizational culture and is performed to fulfill institutional goals. It is organized using rules and delimiters prescribed by the institution. This includes Information Security policies, rules, and standards. However, during the daily work process some situations go beyond the prescriptions, so people, aiming to achieve the task's objectives, need to develop strategies to maintain the workflow, which is often not following the institution's Information Security guidelines. To identify the main factors that generate unsafe behavior, this study proposes a methodology for the analysis of real work situations.

This methodology is based on the Ergonomic Analysis of Work (AET).

5.1 Ergonomic Analysis of Work (AET)

The methodological approach proposed by ergonomics has an inductive research logic, in which the ergonomist goes into the field to produce knowledge. Thus, AET proposes that the investigation take place where the problem is occurring. In this way, it allows a concrete

possibility of transforming work in conjunction with the production of knowledge. The AET method is made up of a set of steps and actions that maintain an internal coherence.

The different techniques are used according to the problem and the configuration of the demand. It is common to use cursive, participative, non-participative, and think-aloud systematic observations. Open, semi-structured, closed, collective, or individual interviews are also used. Open-ended, closed-ended, or survey questionnaires can be used. Other techniques used are document analysis (documents made available by the company), direct measurement with appropriate instruments of the variables that determine the physical conditions of the work environment, and confrontation (returning the collected data/results to the workers).

These techniques are selected according to the nature of the work, the characteristics of its environment, and the objectives of the researcher in several stages of the investigation. The stages of Ergonomic Work Analysis are composed of the following phases:

a) Demand analysis;
b) Collecting information about the company;
c) Survey of the population characteristics;
d) Choice of the situation for analysis;
e) Technical process and task analysis;
f) Global and open observations of the activity;
g) Preparation of a pre-diagnosis - level 2 explanatory hypothesis;
h) Systematic observations - data analysis;
i) Validation;
j) Diagnosis;
k) Recommendations and Transformations.

The present study consists of an ergonomic intervention based on TSA, which was conducted until the stage of elaborating a pre-diagnosis of the work situation. Despite the fact that systematic observations allow a better measurement of the work reality, the present study is understood as exploratory, which aims to identify the main variables associated with unsafe behavior in the work environment. Thus, the diagnosis was developed from the combination of global observations and semi-structured interviews conducted in the work environment. Also, for the understanding of people's behavior, the presence of the ergonomist in the actual work situation during its realization is a determining factor. This presence constitutes one of the fundamental differences between ergonomics and other work-study approaches (ABRAHÃO et al., 2009).

5.2 The Study Design

This work does not propose to make a precise analysis of each of the safety problems identified, but to obtain a general diagnosis of the various problems related to the unsafe behaviors of employees. As a first step in the research, the rules, standards, policies, and recommendations of Information Security (IS) related to the institution were surveyed as a requirement to understand the tasks. Soon after, it was sought to understand the organizational structure of the IAPF. Sequentially the Information Security problems related to insecure behavior, registered in the daily routine of the Information Technology Department (DTI), were surveyed. Finally, it was sought to understand from people's point of view about the reasons for not complying with IS guidelines, what are the real reasons that lead employees to adopt a behavior considered insecure, aiming at its broader understanding. The techniques used in the study were Documentary Analysis of records and information systems available in the

institution, semi-structured interviews with workers, and Participatory Global Observations of employees at the IAPF Headquarters.

The Documentary Analysis occurred to understand the organizational structure and the position of the IAPF on the national and international scene. This information was acquired from the institution's website. Later it was complemented by consulting its Master Plan. Next, the role of the Information Technology Department in the organizational context, as well as its mission, vision, values, and organizational structure were surveyed through the Information Technology Master Plan (PDTI). Also employing the PDTI, information was gathered about the coordinations that make up the DTI, and especially about the department's Service Center. As a complement, the internal regulations of the Department of Information Technology were investigated.

To understand the volume of demands related to Information Technology at the headquarters of the IAPF, it was surveyed in the system that manages the telephony in the IAPF the number of phone calls received monthly by the Central Services. Similarly, through the reports issued by the service registration software, the number of services provided every month was calculated. Through a semi-structured interview with the coordinator of the information systems development area of the DTI, the number of systems developed without permission by administrative departments was obtained. Likewise, an employee of the IAPF library was interviewed about the organizational structure. Also with the help of the work order logging tools, the collaborative writing tool, and the hardware-software inventory, the incidents related to employee behavior in the 15 months before the observation period were collected (the year cannot be identified for security reasons).

The Information Security guidelines of the IAPF were surveyed through the internal norm No. 20, where the e-mail use policy is published, the DTI service instruction, regarding the use of mobile equipment on the local network, and the Information Security Booklet that is published on the intranet. Other IS guidelines were consulted on the website of the Brazilian Court of Audit, such as the Information Security Best Practices Guidebook, the court rulings, and decisions. Likewise, the website of the Information Security Department (DSI) of the Institutional Security Cabinet of the Presidency of the Republic was consulted.

Through the Actual Work Activity Analysis, the behaviors considered unsafe during the work performance of some employees were collected. Participative global observations of people's behavior at the Service Center were recorded over three weeks, parallel to the verbalizations related to incidents caused by unsafe behavior. The Global Observations and the Participative Global Observations took place in the following way: first one employee was chosen per day to make the first contact, in which the researcher presented his or her position and the work developed in the IAPF. Then the objectives of this case study were presented, it was said that he would be observed performing his work for 1 hour and that there could be interventions by the researcher to understand the work and ask questions about his actions. Then, he was invited to participate in the research. At this moment, you were also guaranteed confidentiality about your identity and the data collected. In the cases in which there was an authorization, formalized with a consent form, the observations started immediately and the researcher was seated next to the employee's desk to start the observation. In cases of negative response, the researcher thanked the employee and looked for another employee. During the observations of the work activity at the IAPF headquarters, each behavior that was not appropriate to the institution's Information Security guidelines was recorded. During some actions, interventions were made by the researcher from three pre-formulated questions. The goal was to understand the real reasons that led employees to adopt insecure behavior. At the end of the observations, the employee was allowed to read the record.

It is understood that other steps of AET could be performed to infer and measure the factors related to unsafe behavior, such as the Systematic Observation process. However, due to the exploratory nature of this case study, only the identification of these factors was performed by the combination of global observations and semi-structured interviews.

5.3 Participants' Characteristics

A total of ten people participated in the research. During the document analysis stage, two people helped in the process of surveying and identifying the records. One has a high school degree and works as an administrative assistant, and the other has a college degree and works as a systems analyst. The remaining eight people participated in the research by being observed at their workplace. Of these, four are female. The first one has a medium-level education and works as a secretary. The second has an incomplete college degree and occupies the position of administrative assistant. The third and the fourth have a higher education level and a degree in the humanities.

The positions they hold are in the areas of communication and human resources. Of the four male participants, the first has a college degree in technology and occupies the position of assistant. The second also has a college degree in exact sciences and occupies the position of analyst. The third has a master's degree in systems analysis and holds a position in the technology area of the institution. The fourth and last one has a doctorate in exact sciences.

6 RESULTS AND DISCUSSION

This section aims to present the results obtained in the research and, simultaneously, to proceed with its discussion. The organization adopted begins with the presentation of the incidents recorded in the period. Next, the Information Security incidents directly observed, related to the adoption of unsafe behavior by employees, are emphasized. Subsequently, their difficulties in adopting a secure behavior in their day-to-day work are discussed.

6.1 The Security Incidents

As for the main incidents associated with unsafe behaviors, it was found that the IAPF headquarters does not officially record them. Therefore, to identify them, the Service Center work order registration tool, the computer hardware and software inventory program, antivirus server reports, and semi-structured interviews with DTI employees were used.

The main information security incident related to employee behavior was the sharing of an employee's password with several other people, which resulted in an intern using it to make external calls, including long-distance and "friendship disk" services, as well as accessing pornographic sites. Another five employees suspected that their passwords might be being used by third parties and requested help to change them. Similarly, eight occurrences were registered of users exceeding the storage limit of the local disk of their microcomputer, compromising the storage of institutional information. Likewise, ten cases of local disks of workstations that stopped working, making it impossible to access information and/or its total loss.

According to data extracted from the hardware and software inventory system, during the year of collection at the IAPF, 97 unlicensed office suites were found installed on workstations and later removed. According to the antivirus manager's report, this application needed to be reinstalled on five machines after they were removed by users who have administrative privileges on their microcomputer. All of these were infected by virtual pests

because they were without the program. Of these, in three cases the operating system had to be reinstalled. Still, two other pieces of equipment with administrative rights granted to their users had their operating system reinstalled due to changes in their default configuration. Still, 31 users remain with administrative privileges on their workstations.

According to the coordinator of the DTI systems development area, in the same year, a survey was done for the PDTI of the IAPF, and 15 applications that are in production developed by unauthorized employees from other departments were counted. With this, there were 24 calls to the DTI to solve problems with these applications, such as programming errors, lack of support for a high number of connections, and memory overflow. Furthermore, seven directory shares were removed from user machines that were allowing access to sensitive data. four flash drives presented problems making it impossible to access stored files, two of which were caused by viruses in the device.

For comparison purposes, in the first quarter of the following year alone, there were seven requests to recover corporate data on flash drives and external hard drives, one workstation disk exceeded its storage limit, eight requests to remove viruses from microcomputers, three reinstallations of the operating system, in which users with administrative privileges changed the system's default settings. In addition, three local disks presented a problem that made it impossible to access data, three users performed backups on optical media, and two machines have already had their antivirus reinstalled.

Thus, with these indicators of problems raised during the attendance to the IAPF IT users by the support area attendants, it can be seen that there is a significant number of occurrences generated by irregular behavior related to Information Security. These incidents can compromise the company's Reputation and Reliability concerning the population. They can also cause business discontinuity, in which society is the one who would suffer the most with the loss or delay of its actions or the damage caused to the public coffers.

6.2 The Unsafe Behaviors Observed

According to the objectives of the work, in addition to the main unsafe behaviors registered in the DTI systems, the ones collected through direct observation of the work activity are described. The number of occurrences and the consequences that these behaviors can bring to the institution are also presented. The results are presented in Table 1 and detailed below.

Table 1. Observed unsafe behaviors and related safety problems

UNSAFE BEHAVIOR OBSERVED	QTY.	SECURITY ISSUES
Password Sharing	7	Unauthorized access (confidentiality)
No screen lock when away	6	Theft and unauthorized access (availability and confidentiality)
		Alteration of document content (integrity)
Clean Table Policy	6	Theft and unauthorized access (availability and confidentiality)
		Alteration of document content (integrity)
Use of bottles and glasses with water on the table	5	Unavailability of documents
		Workstation unavailability
Storing corporate data on flash memory media	3	Loss or theft of media (availability and confidentiality)
		Media Failure (availability)
Backup on optical media	3	Loss or theft of media (availability and confidentiality)
		Media Failure (availability)
Using a personal laptop on the local network	3	No update patch control, antivirus program (availability)
		May allow unauthorized access to information (Confidentiality)
Storing files in public directories on workstations	2	Improper access (confidentiality)
		Improper alteration of documents (integrity)
		Undue Exclusion (Availability)
Storing Corporate Data on the Workstation	2	Deletion and corruption of data (availability and integrity)
Development of information systems by unauthorized employees	2	System does not support the number of connections required (availability)
Use of personal e-mail for institutional matters.	2	Message interception (confidentiality)
		There is no guarantee of privacy of the content of the messages. (confidentiality)
Storing personal data in the network driver	1	Lack of resource for institutional data and virus contamination (availability)
Sharing with permissions beyond the required ones	1	Improper access (confidentiality)
Installation of unauthorized programs	1	Fine
		Piracy
		Trojan Horse
Antivirus Removal	1	Virus contamination (availability)
		Unauthorized access to information (confidentiality)
		Unavailability of system and network resources (availability)
Backup routine	1	Failure to restore data (availability and integrity)
Periodic password change	1	Unauthorized access (confidentiality)

Source: field research

The main unsafe behaviors registered in the Information Technology Department throughout the observations were presented. However, the question remains about the reasons

why they are adopted, what were the difficulties and obstacles that employees encounter to comply with the recommendations related to Information Security. Thus, the main difficulties reported by the observed employees in complying with the Information Security guidelines in force in the institution are presented.

6.3 The Difficulties Related to Secure Behavior

In the present section, the difficulties reported by employees in complying with the Information Security guidelines in force in the institution are discussed, organized by categories of problems identified.

6.3.1 Password Sharing

Concerning sharing passwords, of the seven cases observed, five employees claim the need to receive help from other people. The reason is that there is a large amount of work in their sector and little time to do it. According to the employees, generally, the help they receive is from interns and, due to the differentiated form of work contract, they do not have access to the information systems.

In this case, a conflict is perceived between the production norms and the security guidelines of the institution. The employee has many tasks and needs help to perform them, but the institution does not offer support. Consequently, the employees develop strategies to get their work done, which, in this case, consists in sharing the password, which allows unauthorized people to have complete access to the systems. For employees, the work is primary, so if it is not done the consequences will be immediate. Therefore, there may be a prioritization of work objectives over security recommendations. As the guidelines have a preventive character, they tend to take a back seat in the day-to-day work in situations of conflict or time pressure.

Of the five cases reported, one, in particular, is more serious. The employee states that he does not change his password periodically. With this, the trainees, even after they have been disconnected from the company, continue to have the possibility of accessing services and information from outside the institution, since several of them are available on the Internet. He claims that he does not make the switch because it will cause him inconvenience, as he will have to disclose it again to everyone who needs to use it. In this way, the employee has created a work organization in his sector, redistributing the tasks among the trainees, creating work objectives different from the formal assignments. For this organization to work, he cannot change the password.

In the sixth case, the observed employee exclusively performs a certain activity. Thus, to avoid a possible interruption in the workflow when facing unforeseen circumstances, such as medical leave, the strategy is to share the password with one of his superiors. By doing so, he anticipates that other people will be able to perform his activities in an emergency. In this case, a problem may be evident in the organization of work, which has conflicting prescriptions. The work must have a continuous flow, and yet only one person is assigned to perform it.

Predictable situations such as vacation and sick leave were not considered in the task proposal. In addition, the institution's Information Security recommendations suggest that the password be kept confidential. In this case, if this recommendation is met, the workflow should be interrupted. This context of conflict between prescriptions forces the employee to choose between performing the job or complying with the security guideline. Again, a choice based on

the primary character of performing the work was verified, because the consequences will be immediate if it is not performed.

In the seventh and last case of password sharing, the employee states that he is aware of the existing risks when the sharing occurs, However, he claims that, when he arrived at the institution a few months ago, this practice was already common. Because of this, he felt obliged to incorporate this practice in his daily activities and, he also states that he does not know what to do to change this situation.

It can be noticed that the practices of developing operative strategies that do not comply with safety standards due to prescription conflicts have occurred numerous times in the institution and, as a result, an organizational culture of non-compliance with the IS recommendations of the IAPF may have already been generated.

6.3.2 Unauthorized Systems Development and Data Storage

More serious cases were also observed, such as the two employees of an administrative department who were developing applications and using them in the institution without authorization from the Information Technology Department. According to them, the department where they work requested the DTI to develop a system to automate several processes. The DTI claimed that there were several demands in their queue and that the request could only be fulfilled within two years. Faced with the need for the application and the long deadline stipulated by the DTI, the head of this department decided to gather two of his employees and develop the system by himself. In this case, a work organization problem may be triggering several other IS problems. As there are several demands on the Information Technology Department and the amount of personnel is not enough, the demanding parties create strategies to solve their immediate needs. As a result, systems are developed without the DTI's authorization, which is usually poorly planned and out of the institution's standards. These solutions usually do not even support the access and storage demands of a corporate environment.

The development of programs by employees of administrative departments also generates other Information Security problems, such as the backup routine. Besides being manual and not being tested periodically, the backup tape is stored in the developers' room. One of the employees was questioned about the risks of storing the tape under these conditions. He replied that he was aware of the dangers and that he intended to remove the tape from that room and store it on another floor of the building.

From these reports, it is understood that the work organization problem triggered several other problems. In this sense, the lack of people in a certain sector led the DTI not to accomplish its tasks and forced the other departments to create their strategies to solve the problem, affecting several aspects of institutional Information Security.

In addition, on the local network at the IAPF headquarters, each department has a reserved space on the network servers to store and share files, they are better known as network drivers. These locations receive a daily backup routine, which ensures the availability of the files stored there. Two other employees were observed saving their corporate data to the local disk of their workstations instead of using the network disk. When asked about this practice, one of the employees reported that in cases of network unavailability, the data will remain accessible because it is stored on his microcomputer. The second stated that part of the files he generates are saved on the network driver, but that he does not keep all the files there because he has received notifications that he exceeded the storage limit a few years ago.

In the case of the first employee, it is understood that the unsafe behavior is caused by the unreliability of the institution's local network. For him, a sudden stop in the network will prevent him from doing his work. For this not to happen, he elaborates the strategy of storing the files on his microcomputer, with this he declares that he has the feeling of being safe.

The second case is related to the lack of working conditions. The employee does not have enough space on the network driver to store all the necessary files. This lack leads the employee to devise the strategy of sorting the files and storing them up to the disk limit. Another problem is also noticeable, the lack of information. The IAPF headquarters has increased its storage capacity in recent years and now there is no longer the problem of lack of disk space. However, the employee continues with the old information, maintaining the strategy to avoid space problems.

In two cases, employees were seen storing corporate data on their workstations in places of public access. Questioned about the behavior, one claimed to be unaware of the possibility that other people could access the data stored on his microcomputer. For him, the data was safe. The second, on the other hand, declared that he saves the data outside his profile to facilitate searches because he has developed his directory structure that speeds up his work.

In the first case, the insecure behavior adopted by the employee may have causes such as lack of technical knowledge or ignorance of security guidelines. To store the data on the workstation he lacked technical knowledge. So to act, he evoked other knowledge that had been significant to him in similar situations, aiming to try to solve the problem, which led him to use a non-recommendable place for storage. The knowledge evoked by this employee did not contemplate the Information Security recommendations, and this may have been caused by a lack of knowledge or lack of training. If he does not know the security guidelines, he will not consider them in his actions. If he has been trained, this may not have been fixed and, because it is not part of the routine, it was not remembered.

In the second case, we notice that the microcomputer interface is not adapted to the employee's representations, that is, the directory structure makes it difficult to locate information. Therefore, he elaborates the strategy of creating an alternative structure model according to his experiences, which makes it easier to manage the information. However, the system's file structure is inflexible causing him to disregard the recommendations to create a structure more suitable to the representation of his mental model.

As for the storage of personal files on network disks, one employee was observed keeping personal music, photos, and videos there, occupying the space that is destined for institutional files. He stated that he knows the backup routine that is performed daily on the network disks and that, as he would not like to lose any of his files, he decided to store them in this location. In this case, for the employee, there was a risk that the files would be lost, and his goal was to keep them safe, available, intact. Using the information that the files stored on network disks have a daily backup routine, he takes advantage of this institution's production rule and stores his files on the network. In this way, he keeps his files much safer than on any other storage medium available at his workstation. Thus, the employee devises a problem-solving strategy without taking into consideration that his behavior jeopardizes the security of institutional information because the spaces reserved for institutional files are occupied by personal files.

6.3.3 The Clean Table Policy and File Sharing

In the cases where four people kept documents on the desk during their absence from the room and did not block the microcomputer screen. When asked about the risks of files and

documents being stolen, altered, and deleted, two responded that they trust the people who work around them, and that they have never had problems related to these cases. Despite this, they stated that they are aware of the dangers regarding unknown people visiting their room. One employee stated that he forgot only during the time he was being observed, but that he usually keeps his desk clean, cabinets and drawers locked, and screen locked. The last one stated that he keeps the documents and locks the screen of his workstation only during the times he considers longest, such as lunch time and the end of the workday, because for him this is the period of greatest risk.

In these cases, it is noticeable that employees use the strategy that gives them the least effort. For them, putting the documents away every time they leave the workstation and returning them to the desk when they return increases their workload. By the employees' reports, the incidents with these documents are low, and there is trust among the people around them. There are also no official records in the institution about these cases, for this reason, the chosen strategy is the lighter workload. With this, they channel their efforts to other activities.

About the sharing of sensitive files, an employee kept in his workstation a directory with confidential files (internal audit) that had access permissions beyond the necessary ones. This made it possible for all users on the local network to access the contents of this directory. Questioned about the access permissions, the employee informed that he needed to share some files with some employees, and that when doing so, he chose only the default system options. The user verbalized that he did not imagine that such action was allowing any network user to access the directory's content.

This fact leads us to realize that the employee elaborated an inadequate security strategy to solve the problem. He had files on his workstation and needed to share them with some people in his sector. When analyzing the possibilities to solve the problem, he verified that sharing through the local network is the most viable. So, the employee performs the share action and uses the system's default options, thus allowing everyone on the local network to access the content. The employee considered that the problem was solved, and did not realize that he was also generating an information security problem. The system interface may have influenced when it did not inform clearly that such action would make the files available to all employees and consisted in an operation with security risks.

6.3.4 Use of Personal Equipment on the Local Network and Use of Private E-mail

Three personal laptops were also found accessing the local network. According to one of the employees, the reason is related to the fact that he develops applications for his department and, as the institution does not have a license available for a certain software, he uses his equipment that has a copy of the license. The unsafe behavior of this employee is generated by a flaw in the working conditions offered by the organization. He has the task of developing a computer program, but for this, he needs a tool that is not officially available from the institution. Thus, he elaborates the strategy of bringing his equipment to the institution and accomplishes his work objectives. The lack of working conditions leads the employee to adopt an insecure behavior. It is worth mentioning that, to perform this work, the institution proposes the use of another tool, with lower productivity potential, which increases the employee's workload.

The second user argued that he always used his notebook on the network and that this facilitates his work, providing mobility and agility in performing his activities. In this case, the employee received a microcomputer from the institution, but prefers to use the notebook, and

argues that the lack of mobility generates a great impact on his workflow because the information and systems contained there are essential for the fulfillment of his work objectives.

The third employee explained that, according to his duties, he must perform activities both in the IAPF headquarters building and in a data collection field. Thus, he is required to use a mobile device for his work. However, according to his statement, his department does not have similar equipment. Therefore, he uses his own equipment. In this third case, the lack of work tools causes unsafe behavior, because the nature of the task requires mobility so that data and systems are available at both workstations.

In two other cases, the use of private e-mail for institutional matters was observed. According to one of the employees, there are constant problems with the availability of corporate email and the attachment size limit. For this reason, he uses five different private email accounts, together with the institution's email, to send electronic messages. The second employee affirms that he uses his private email during the unavailability of the service or when he has problems receiving messages on the corporate email.

It can be seen that in both cases the unreliability of the e-mail system at the IAPF headquarters leads employees to adopt unsafe behavior. They use their private e-mail for corporate matters. In the first case, there is also the problem of inadequate working conditions, because the employee needs to send files attached to the message that are larger than the limits allowed by the system. As a result, he uses private e-mail as a way of achieving the objectives of his task.

6.3.5 The Use of Flash Memory Devices and File Backup

Of the three employees observed that store institutional data on flash memory and hard disk devices, two responded that they keep copies of data they deem important on these devices. When asked if they were familiar with the network disk and the daily backup routine, they replied that they are, but that when using these devices, they feel safer. Another employee replied that he handles a very large amount of data and when he uses the network the file transfers are time-consuming. By using this device, he speeds up his activities.

In the first two cases, it is noticeable the lack of reliability in the backup system and the local network of the IAPF Headquarters, so they develop strategies to store institutional data on these devices and have the feeling of being safe against any unforeseen event. In the third case, the lack of time leads them to elaborate a strategy that will speed up their work. In the three cases presented, unreliability and time pressure cause employees to adopt unsafe behaviors.

In addition, three users were observed backing up to optical media. One claimed that the amount of data he handled was too large to put on a network driver and that it would take too long. A second employee argued that he was concerned that the data would be lost if there were a problem with the local disk at his workstation. So he used the strategy of storing the backup on optical media since his computer has a CD burner. Asked if he knew the network driver, the user replied that he did not. After being enlightened about the existence and functioning of the driver, he said he would start using this resource. The third alleged that his microcomputer would be replaced and was apprehensive about the possibility of losing some data during the change.

In the first case, it is again understood that the organization of work exerts time pressure on the employee. With this, he adopts the strategy of storing the data on a flash memory disk without worrying about the insecurity that this behavior brings to the information. The second one, on the other hand, distrusts the institution's information systems and decides to

record the information in a flash memory device. The third states that the lack of knowledge of institutional resources causes insecure behavior.

6.3.6 Use of Software Without the Proper License

In the case of the user who uses a program without the proper license, he reported that he has administrative privileges on the computer and that he installed an unlicensed copy of the product because he claimed to have more skills in using this product than the one offered by the institution. In this case, the employee's strategy is the one that brings him less workload and more flexibility. Since his primary goal is to perform the task, he disregards the security policy, which is preventive and does not cause immediate consequences.

Finally, an employee, who also has administrative privileges on an institution notebook, had removed the antivirus program from the equipment. When questioned about this behavior, he stated that the antivirus was slowing down the system and this was preventing him from working. It can be seen in this case that the employee's primary goal was again to get his work done. Since for him the antivirus was hindering his activities, he elaborated the strategy of removing it and getting the job done. Since the antivirus was only preventive he chose to take the risk of a virus attack and get the job done.

6.3.7 Initial Diagnosis

Once the analysis of the actual work of the IAPF employees has been performed, the existence of unsafe behavior that has put the Institution's Information Security at risk is verified. Moreover, it is evident that most of the cases of unsafe behavior that were observed stem from the lack of planning of work organization, the lack of an institutionalized Information Security Policy, the lack of knowledge of the current Information Security guidelines, the conflict between security prescriptions and rules, time pressure and practical conditions to perform the work. These problems lead employees to devise strategies that maintain the flow of work to the detriment of security rules.

It can be seen that all strategies, even if they put the institution's information security at risk, are focused on the execution of work activities. The work is prioritized because if it is not done, it will have immediate consequences. The security guidelines, on the other hand, are preventive, their consequences are not always immediate and, therefore, they are not taken into consideration in the elaboration of work strategies. These strategies appear positive in the short term, but in the long term, they generate losses for the institution, such as the redirection of the workload of other employees to solve the security problems created security incidents, and effects on the employees' well-being.

In many cases, the people responsible for developing the Information Security guidelines in the institution are different from those who organize the work, and this creates dissonance between the objective of the people's work and the security prescriptions. It is understood that the end goal of the organization is not the security itself, but the production and management of knowledge. In this sense, the guidelines need to come as a means of supporting the institutional objectives, and not in the opposite way. For this, it is understood that it is necessary that those responsible for developing information security guidelines better understand what is done by the employees in each sector to perform their work to generate standards, rules, and procedures that are more appropriate to the institution on an ongoing basis.

7 FINAL CONSIDERATIONS

The present study identified the main factors related to unsafe behavior at the IAPF Headquarters. Factors already predicted in the Information Security literature were identified, such as the lack of an Information Security Policy, the lack of knowledge of the Information Security recommendations in force. Also, a possible conflict between the support for carrying out the work and the prescriptions of the Information Security guidelines was verified. Other factors that may also influence insecure behavior, such as targets for attackers who exploit employees' need for personal benefits, for example, were not identified. To this end, a research approach originating in Ergonomic Analysis of Work was used, focusing on the comparison of work prescriptions and their practical execution.

The study was limited to showing only an overview of the main factors related to unsafe behavior. Limitations of the research are considered to be the short time available for its realization, which reconciled the researcher's working hours with data collection, the difficulties in finding people in the institution willing or available to contribute to the research, and situations of lack of physical space for the accommodation of the researcher during observations. Another factor that limited the depth of the study was the difficulty in obtaining accurate data from the institution's computerized systems, such as Information Security incidents and accidents since they are not officially registered. The lack of the official Information Security Policies document was also identified. Moreover, because it is a work that involves sensitive information, some information had to be omitted so as not to compromise the Institution's Security. Another yes, the Information Technology Department is in a restructuring process. This transition moment has made it difficult to accurately report its structure and flows, as there are currently many undefined processes.

However, it is believed that, despite being the first study, the present work points to an issue that demands further deepening in the literature: the conflict existing in the work prescription itself. This may be one of the factors responsible for the difficulty of people to behave safely in Brazilian public institutions. With this, it is avoided that the responsibility for such behavior falls only on individuals, eliminating only the symptoms and not the real focus of the problem. In this sense, we realize that new studies, using the ergonomic approach, will enable a new way to understand the role of the conception of Information Security policies, norms, standards, and procedures, which will allow us to understand how people behave in the real work situation.

Given the reality that organizations have become increasingly dependent on the availability, secrecy, and integrity of information to increase the efficiency of their operations, the search for protection mechanisms, such as technological tools and methodologies, has become fundamental. Further studies on insecure behavior can produce more evidence so that, in the future, a new approach can emerge for the development of Information Security guidelines that take into account the real needs of people in the work situation, promoting the creation of a security culture.

CRediT

RECOGNITIONS: Not applicable.
FINANCING: Not applicable.
INTEREST CONFLICTS: The authors certify that they have no commercial or associative interest that represents a conflict of interest in relation to the manuscript.
ETHICAL APPROVAL: Not applicable.
AVAILABILITY OF DATA AND MATERIAL: Not applicable.
AUTHORS 'CONTRIBUTIONS: Conceptualization, Data Curation, Formal Analysis, Investigation, Methodology, Project Management, Resources, Visualization, Writing – original draft: Santos, R.B.; Pontes e Silva, T.B.; Writing – revision & edition: Pontes e Silva, T.B.

REFERENCES

ABRAHÃO, Júlia Issy. **Reestruturação produtiva e variabilidade do trabalho:** uma abordagem da ergonomia. Psicologia: Teoria e Pesquisa, Brasília, Vol. 16 n. 1, p. 49-54, jan/abr. 2000.

ABRAHÃO, Júlia Issy; PINHO, Diana Lúcia Moura. **Teoria e prática ergonômica**: seus limites e possibilidades. Em: M. G. T. da Paz & A. Tamayo (org.), Escola, saúde e trabalho: estudos psicológicos. Brasília, Universidade de Brasília. p. 229-239. 1999.

ABRAHÃO, Júlia Issy; SZNELWAR, LAERTE; Silvino, ALEXANDRE Magno Dias; SARMET, Mauricio Miranda; PINHO, Diana Lúcia Moura. **Introdução à ergonomia**: da prática à teoria. Brasília: Edgard Blucher, 2009.

ALBUQUERQUE, Ricardo; RIBEIRO, Bruno. **Segurança no desenvolvimento de software:** como desenvolver sistemas seguros e avaliar a segurança de aplicações desenvolvidas com base na ISO 15.408. Rio de Janeiro: Campus, 2002.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **NBR ISO/IEC 27002**: Tecnologia da informação - Técnicas de segurança - Código de prática para a gestão da segurança da informação. Versão 2. Rio de Janeiro, 2005.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27001** Tecnologia da informação - Técnicas de segurança - Requisitos. Rio de Janeiro, 2006.

ASSOCIAÇÃO INTERNACIONAL DE ERGONOMIA - IEA **O que é ergonomia.** Available at: https://iea.cc/what-is-ergonomics/. Access on: 29 junho 2020.

BALLONI, Antônio José. **Por que gestão em sistemas e tecnologias de informação?** Segurança, inovação e sociedade. São Paulo: Komedi, 2007.

BRASIL. **Decreto nº 9.637, de 26 de dezembro de 2018**. Dispõe sobre a governança da segurança da informação e institui a Política Nacional de Segurança da Informação (PNSI). Brasília, 2018.

BRASIL. Presidência da República/Gabinete de Segurança Institucional. **Portaria nº 93, de 26 de setembro de 2019**. Aprova o Glossário de Segurança da Informação. Brasília, 2019.

BRASIL. Tribunal de Contas da União. Secretaria de Fiscalização de Tecnologia da Informação. **Boas práticas em segurança da informação.** Brasília, DF, 2008. 70 p.

CERT.BR: **Estatísticas dos incidentes reportados ao Cert.br**. Disponível em http://www.cert.br/stats/incidentes. Access on: 10 de fev. 2010.

CHIAVEGATTO, Myrza Vasques. **A gestão da informação e o processo decisório na administração municipal de Belo Horizonte**, Informática Pública, Belo Horizonte: v. 2, n. 2, p. 53-57, dez 2002.

DIAS, Cláudia. **Segurança e auditoria da tecnologia da informação**. Rio de Janeiro: Axcel Books, 2000.

FERNANDES, Jorge Henrique Cabral. **Introdução à gestão de riscos de segurança da informação.** Texto desenvolvido para suporte às atividades de ensino do programa de pesquisas e Formação de Especialistas para Elaboração da Metodologia Brasileira de Gestão da Segurança da Informação e Comunicações, do módulo Gestão de Riscos de Segurança I. Departamento de Ciência da Computação. Universidade de Brasília. 81 p. 2009.

FERREIRA, Mário César. **Atividade, categoria central na conceituação de trabalho em ergonomia.** Revista Aletheia, Canoas, RS, n. 11, p. 71-82, 2000.

FONTES, Edison Luiz Gonçalves; BALLONI, Antonio José; LAUDON, Kenneth. **A segurança de sistemas da informação: aspectos sociotécnicos**. 2015.

FRÓIO, Leandro Ramalho. **Um modelo faseado de gestão da segurança da informação.** 2008. 134 f. Dissertação (Mestrado em Engenharia Elétrica) Departamento de engenharia elétrica, Universidade de Brasília, Brasília, 2008.

LOPES, Ângela Cristina Figueiredo. **Segurança da informação versus prontuário eletrônico:** hospital geral de Fortaleza – CE. 2009, 49 f. Monografia (especialização em aplicações complementares às ciências militares), Escola Superior do Exército. Rio de Janeiro, 2009.

MASLOW, Abraham Harold. **Motivation and personality**. New York: Harper.1954.

NETTO, Gilberto FREIRE, Pedro; ALLEMAND, Marcos. **Gestão operacional de segurança da informação.** Texto desenvolvido para suporte às atividades de ensino do programa de pesquisas e Formação de Especialistas para Elaboração da Metodologia Brasileira de Gestão da Segurança da Informação e Comunicações, do módulo Gestão Operacional de Segurança da Informação. Departamento de Ciência da Computação. Universidade de Brasília. 50 p. 2008.

PELTIER, Thomas. **Information security policies and procedures:** a practitioner's reference. 2. Ed. Auerbach Publications, Flórida, 2004.

SÊMOLA, Marcos. **Gestão da segurança da informação: uma visão executiva**. Rio de Janeiro: Campus, 2003.

SILVINO, Alexandre Magno Dias; ABRAHAO, Júlia Issy; SARMET, Mauricio Miranda. **Ergonomia, cognição e trabalho informatizado.** Psicologia: Teoria e Pesquisa, Brasília, vol. 21, n. 2, p.163-171, 2005.

SILVINO, Alexandre Magno Dias; ABRHAO, Júlia Issy. Navegabilidade e inclusão digital: navegabilidade e competência. **Revista de Administração de Empresas**, São Paulo, RAE-Eletrônica. v. 2, jul/dez 2003.

SILVINO, Alexandre Magno Dias. **Ergonomia cognitiva e exclusão digital:** a competência como elemento de (re)concepção de interfaces gráficas. 2004, 193 f. Tese (Doutorado em Psicologia), Universidade de Brasília, Brasília, 2004.

SIMON, Imre. **A revolução digital e a sociedade do conhecimento**: o que é informação? como ela age? 1999 Available at: http://www.ime.usp.br/~is/ddt/mac333/aulas/tema-11-24mai99.html. Access on: 18 jan. 2010.

SHIREY, Robert. **RFC 2828: internet security glossary**. the internet society, 2000. Available at: http://www.ietf.org/rfc/rfc2828.txt?number=2828. Acessado em: 15 fev. 2010.

STAIR, Ralph. **Princípios de sistemas de informação**: uma abordagem gerencial. Rio de Janeiro: LTC, 1998.

turnitin
Article submitted in the similarity system
Submitted: 03/05/2021 – Accepted: 16/09/2021 – Published: 30/09/2021