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

10.20396/rdbci.v0i0.8646416

INFORMATION SECURITY IN ACADEMIC LIBRARIES: THE ROLE OF THE LIBRARIAN IN PLANNING AND INTRODUCING NEW INSTITUTIONAL POLICIES

SEGURANÇA DA INFORMAÇÃO EM BIBLIOTECAS UNIVERSITÁRIAS: A ATUAÇÃO DO BIBLIOTECÁRIO NO PLANEJAMENTO E NA IMPLANTAÇÃO DE NOVAS POLÍTICAS INSTITUCIONAIS

SEGURIDAD DE LA INFORMACIÓN EN BIBLIOTECAS DE UNIVERSIDAD: LA INTERPRETACIÓN DEL BIBLIOTECARIO EN LA PROYECCIÓN Y EN LA INTRODUCCIÓN DE NUEVA POLÍTICA INSTITUCIONAL

Juliana Soares Lima[1], Ana Rafaela Sales de Araújo, Francisco Edvander Pires Santos, Luiz Gonzaga Mota Barbosa, Izabel Lima dos Santos
[1]Universidade Federal do Ceará

Correspondência

[1]Juliana Soares Lima
Universidade Federal do Ceará
Fortaleza, CE.
E-mail: juliana.lima@ufc.br
ORCID: http://orcid.org/0000-0001-9399-673X

Submitted: 31-08-2016
Accepted:17-01-2017
Published: 18-04-2017

JITA: LH. Computer and network security.

RESUMO: Apresenta uma discussão sobre a atuação do bibliotecário como um profissional importante no planejamento, na elaboração e na implantação de uma Política de Segurança da Informação em Bibliotecas Universitárias, trabalhando em conjunto com os profissionais da área de Tecnologia da Informação. Discorre acerca das principais pragas virtuais existentes que tendem a infectar os computadores das bibliotecas. Ratifica, tendo como base a legislação vigente e documentos normativos, a importância do bibliotecário estar inserido nas principais tomadas de decisão referentes à segurança da informação, tais como o planejamento de uma Política de Segurança da Informação consistente e que supra as necessidades das Bibliotecas Universitárias como instituições propensas a ataques virtuais. Expõe, com base nos resultados alcançados por meio de pesquisa-ação, os principais tópicos e diretrizes que devem constar numa Política de Segurança da Informação, tendo em vista os problemas encontrados nos computadores das bibliotecas e a análise de conteúdo de relatórios elaborados a partir do preenchimento de formulários nas visitas. Conclui que Política de Segurança da Informação deve ser validada pela gestão e pelos setores competentes dos departamentos e/ou divisões aos quais as Bibliotecas Universitárias estejam hierarquicamente subordinadas.

PALAVRAS-CHAVE: Segurança da informação. Biblioteca universitária. Políticas de segurança.

ABSTRACT: This study presents a short discussion about the role of the librarian as a mediator at planning, developing and implementing an Information Security Policy in Academic Libraries, by working together with professionals in the field of Information Technology. It also discusses the main virtual threats and some risks that are prone to infect computers in libraries. Based on the current legislation and on some normative documents about information security, it is confirmed the importance of the librarian take part in the main decision-making related to information security, such as planning a consistent Information Security Policy which be able to see the specific needs of Academic Libraries as institutions prone to cyberattacks. The main topics and guidelines to carry out an Information Security Policy are presented based on the results that were obtained through an action research, by visiting libraries to fill in application forms and to compose reports whose content was analyzed. Finally, the study concludes that Information Security Policy must be validated by managers of sectors or departments which the Academic Library is hierarchically subordinate to.

KEYWORDS: Information security. Academic libraries. Security policies.

RESUMEN : Presenta una discusión sobre la actuación del bibliotecario como un profesional importante para la planificación, desarollo y la implatación de una Política de Seguridad de la Información en Bibliotecas de Universidades, que trabajan en conjunto con profesionales en el campo de la Tecnología de la Información. Habla sobre las principales amenazas virtuales existentes que proponem infectar los ordenadores en las bibliotecas. Teniendo por base la legislación corriente y los documentos normativos, la importancia del bibliotecario és introducida en las principales tomas de decisiones relacionada con la seguridad de información, como la planificación de una Política de Seguridad de la Información consistente y que suple las necesidades de las Bibliotecas de Universidades como instituciones propensas a los ataques virtuales. Con base en los resultados alcanzados a través de invertigación-acción, expone los principales temas y reglas que deben mostrarse en una Política de Seguridad de la Información, visando los problemas encontrados en los ordenadores de las bibliotecas y análisis de los contenidos de informes elaborados, seguidos de formularios llenados en invitaciones. Concluye que la Política de Seguridad de la Información debe ser validada por la dirección y los sectores relevantes de los departamentos y divisiones los cuales las Bibliotecas de Universidades son jerárquicamente subordinadas.

PALABRAS LLAVE: Seguridad de la información. Bibliotecas académicas. Políticas de seguridad.

1 INTRODUCTION

The satisfaction of the informational needs of each individual user is important both in the traditional form of attendance (in person) and in the form that is required (virtually) in the daily life of Academic Libraries (BUs). Therefore, it becomes extremely important to control and reduce technical incidents and security, among other factors, in order to ensure the operation of the network at acceptable levels of performance as well as to keep your computer equipment with specialized software and applications to facilitate the communication and optimize the flow of information and knowledge, thus allowing the increase of efficiency and conditions of excellence of the information stored in the system used by the libraries, whether in the field of research, teaching, extension, services or institutional management.

In order to highlight the above scenario, it is agreed that:

> Key to understanding the problems that exist in computer security is a recognition that the problems are not new. They are old problems, dating from beginning of computer security (and, in fact, arising from parallel problems in the noncomputer world). But the locus has changed as the field of computing has changed. Before the mid-1980s, mainframe and mid-level computers dominated the market, and computer security problems and solutions were phrased in terms of securing files or processes on a single system. With the rise of networking and the Internet, the arena has changed. Workstations and servers, and the networking infrastructure that connects them, now dominate the market. Computer security problems and solutions now focus on a networked environment. However, if the workstations and servers, and the supporting network infrastructure, are viewed as a single system, the models, theories, and problems statements developed for systems before the mid-1980s apply equally well to current systems. (BISHOP, c2003, Preface, p. XXXIII).

In this context, we intend to carry on a discussion of information security in the environments of the BUs, aimed at inserting the librarian as another acting professional in major decision-making with regard to proposing suggestions, improvements, troubleshooting and / or guidelines to guide access to computers of the BUs, as well as the creation of a security policy of targeted information for these environments. In addition, the librarian has another challenge related to the issue of information security, which is to provide and guarantee free access to the Internet. However, how to reach a consensus or a compromise on an issue that causes controversy and divides opinions among professionals themselves? Regarding this issue and based on the findings made in the work environment that enabled this study, IT professionals deal much better with the problem, considering that the topic is part of their methodology and within it there are proposals for imposing access control measures to better match the use of available resources and computers.

The International Federation of Library Associations and Institutions (IFLA) and the United Nation Educational, Scientific and Cultural Organization (UNESCO) have developed the Guidelines for the Internet Manifesto in 2006, a document that is the starting point, published in 2002, which has been providing wide and useful guidance ever since. However, it is necessary to consider the fact that, since that time, the scenario of Internet, users and

information security has changed considerably. In fact, even the Guidelines that were developed in 2006, which have been translated into other languages and endorsed by IFLA, present some recommendations that have remained the same since that period. Therefore, the topic is extremely opportune for discussion in a period of changes in the Internet and its users, as well as the various regulatory frameworks that have been emerging and generating new clashes.

As an example, there is Law 12.965, dated April 23, 2014 known as the Internet Civil Registry. This law is the initiative of the Federal Executive Branch and aims to establish "[...] principles, guarantees, rights and duties for the use of the Internet in Brazil" (BRAZIL, 2014). The Internet Civil Registry has the challenge of contributing to the construction of "[...] an internet that is viable, accessible and fair for all". (NAZARENO, 2014, p. 27), and precisely for this reason it intends to establish the rights and the responsibilities that all subjects (users, content providers, connection providers, copyright owners and government) related to the Internet in the country. The Internet Civil Registry makes clear the need to establish parameters for the secure access of content available on the Web, and these parameters should not only exist at the national level, but also at the local institutional level, through actions that stimulate information security.

The Internet Governance Committee in Brazil (CGI.br) ([2016]) maintains within its website an exclusive section for the discussions about the Internet Civil Registry, which emphasizes that the security, stability and resilience of the Internet must be fundamental objectives of all stakeholders in Internet governance; therefore, Internet must be a stable, resilient, secure and reliable environment. In addition, it clarifies that the effectiveness of addressing the risks and threats to the security and stability of the Internet depends on strong cooperation among different actors.

In this sense, the development of this study was made necessary not only to establish guidelines for the use and maintenance of computers and for access to the Wi-Fi network of the libraries where an action research was carried out, but also with the purpose of contributing with a proposal of Implementation of an Information Security Policy (PSI) for the Library System of the Federal University of Ceará (UFC), thus meeting the International Standards for Information Security in Libraries (ISO 27001 and ISO 17799). Objectives set out in the Institutional Development Plan (PDI) of the designation (UNIVERSIDADE FEDERAL DO CEARÁ, 2012). It is important to emphasize that information security goes far beyond simple maintenance and diagnosis of computer problems, although this is a problem that involves an area and a consequent discussion about the document, after all, much of the information generated in these environments comes from Computers, as will be seen below.

2 MAIN CONCEPTS AND THE IMPORTANCE OF INFORMATION SECURITY IN INSTITUTIONS

Aiming at the proposal of insertion of the librarian as a professional involved in the planning, elaboration and / or implementation of institutional policies focused on information security, it was necessary to use the theory, some of the existing normative documents and the current legislation on the importance of the information security in institutions, and also on the main malware to which all computers are susceptible. Allied to this, we will discuss the principles and the definition of the Information Security Policy.

In the context of information security, information is an essential asset from the business point of view of an organization and, accordingly, it must be properly protected (ABNT NBR ISO / IEC 27002, 2013). In this sense, Mandarino Júnior (2010) conceptualizes information as an intangible, intangible and volatile good, and its assets become the main focus of information security attention. Examples of information assets are: the storage, transmission and processing of information; the necessary equipment; the systems used; the places where these means are located and the human resources that have access to them (MANDARINO JÚNIOR, 2010).

Information can be considered the most valuable asset for private companies and for public agencies, as well as the most critical resource asset, because when adulterated, unavailable or accessed by people in bad faith without the proper authorization, or by competitors, the image of the institution can be significantly compromised, as well as the progress of the institutional processes themselves, that is, the continuity of an organization can be compromised if due attention is not given to the security of its information (BRASIL, [2014]). It is then considered that:

> In the information society, while information is considered to be the main asset of an organization, they are also at constant risk as never been before. Thus, information security has become a key point for the survival of the institutions. (BRASIL, 2007, p. 2).

By its expressive value, information represents great power to whoever owns it. Moreover, it is integrated with the processes, people and technology. To reinforce the importance of information as a valuable asset and strategic resource for private companies and public institutions, under the vision of competitive advantage, Figure 1 illustrates this reality well:

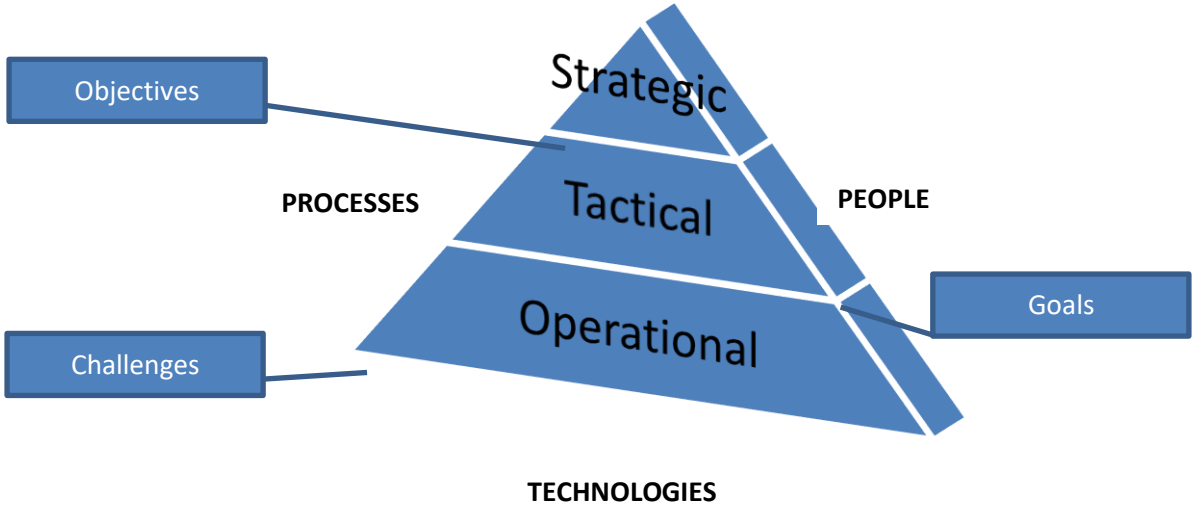

FIGURE 1. Strategic role of information

Source: Authors, based on Rezende and Abreu (2003).

From the understanding of these levels of management and responsibilities, and for this discussion to be carried forward, the term "information security" must be conceptualized. According to Article 2, item II, of Decree No. 3.505, of June 13, 2000, information security is defined as:

> [...] protection of information systems against denial of service to authorized users, as well as against intrusion, and unauthorized modification of data or information, stored, processed or in transit, including security of resources Human resources, documentation and material, communications and computing areas and facilities, as well as those aimed at preventing, detecting, stopping and documenting any threats to its development. (BRASIL, 2000, online).

It is precisely in this scenario that information security is more than necessary in institutions, not only to guarantee secure access and availability of information, but also to comply with the legislation established by the Office of Institutional Security of the Presidency of the Republic through the Department of Information Security and Communications. There is also the Information Security Management Committee, which assists the Office of Institutional Security of the Presidency of the Republic. The Information Security Management Committee is composed of representatives of the Federal Public Administration (BRASIL, 2016): Ministry of Justice and Citizenship; Defense Ministry; Ministry of Foreign Affairs; Ministry of Finance; Ministry of Labour; Ministry of Health; Ministry of Industry, Foreign Trade and Services; Ministry of Planning, Development and Management; Ministry of Science, Technology, Innovation and Communications; Civil House of the Presidency of the Republic; Ministry of Mines and Energy; Ministry of Transparency, Inspection and Comptroller General of the Union; Advocacy-General of the Union; and Secretariat of Government of the Presidency of the Republic; the work is coordinated by the Office of Institutional Security of

the Presidency of the Republic, in the capacity of Executive Secretariat of the National Defense Council.

The existence of each of these bodies guides and validates the actions for the security of information in institutions, among them the Academic Libraries. However, there is no point thinking in an Information covering the environment of Academic Libraries Security Policy is not known, although superficially, the main security concepts of information and its importance, why should we care and what are the types of malware and internal and external threats to which the Academic Libraries are susceptible.

2.1 Information Security Principles and Policy

One of the most complete concepts on information security is presented by Bishop (c2003, Preface, p. XXXII-XXXIII):

> [...] computer security is not just a science but also an art. It is an art because no system can be considered secure without an examination of how it is to be used. The definition of a "secure computer" necessitates a statement of requirements and an expression of those requirements in the form of authorized actions and authorized users. (A computer engaged in work at a university may be considered "secure" for the purposes of the work done at the university. When moved to a military installation, that same system may not provide sufficient control to be deemed "secure" for the purposes of the work done at that installation.). How will people, as well as other computers, interact with the computer system? How clear and restrictive an interface can a designer create without rendering the system unusable while trying to prevent unauthorized use and access to the data or resources on the system? Just as an artist paints his view of the world onto canvas, so does a designer of security features articulate his view of the world of human / machine interaction in the security policy and mechanisms of the system. Two designers may use entirely different designs to achieve the same concept.

Therefore, based on the above, it can be considered and summarized in general terms that, for the creation of any Information Security Principles and Policy it is mandatory to present criteria and / or guidelines of what can and cannot be done in the computers and through the network used, in addition to defining who can use and how to use these equipment and resources.

According to Concerino (2005, p. 155), information security has three basic pillars. Presenting them in general terms, they are:

a) Confidentiality: refers to the confidentiality of information. It seeks to ensure that information is accessible only to duly authorized persons. When some information is seen or copied by someone who is not authorized to do so, this aspect of security is not being observed;

b) Integrity: refers to the inability to change information on the network. It aims to safeguard the data and information, thus ensuring the veracity and authenticity of the information, as well as its processing methods. The loss of integrity occurs when, lacking due

security, the modification of an important topic occurs, which can be altered by the most surprising motives, even intentionally;

c) Availability: seeks to ensure that data, information and systems will be fully available whenever requested. The absence of availability occurs when the information is deleted or becomes inaccessible to the user authorized to consult it.

In the literature of the area, there are more principles related to information security, however, for the purposes of this study, only the three mentioned above were considered.

The classification of information in organizations must be carried out in order to ensure that information is given an adequate level of protection, according to its importance. Each institution should label and handle the information in accordance with its own classification scheme (ISO / IEC 27001, 2013). Based on this classification, the classified documents we have, composed of data or information whose unrestricted knowledge or disclosure may result in any risk to the security of society and the state, as well as those necessary to guard the sanctity of their privacy, honor And the image of people. This type of information and document should receive special security measures (BRAZIL, 2011).

On the other hand, ostensible information is characterized by being easily perceived and understood, sparing no effort in its assimilation. In this sense, Decree No. 5,903, dated September 20, 2006, establishes and regulates, based on Laws No. 10,962 and No. 8,078, infractional practices that address the consumer's basic right to obtain adequate and clear information about products and services. (BRASIL, 2006).

The information security booklet prepared by the Superior Court of Justice clarifies that:

> An agency that takes Information Security seriously keeps the risks and threats under control and does not put its organizational image at stake. With this, the entire institution gains and maintains its highest objective: to provide a quality service for the Brazilian citizen. (BRASIL, [2014], p. 16).

Complementing the recommendation of the booklet, according to Bishop (c2005), the author clarifies that:

> [...] the Internet provides only the most rudimentary security mechanisms, which are not adequate to protect information sent over that network. Nevertheless, acts such as the recording of passwords and other sensitive information violate an implicit security policy of most sites (specifically, that passwords are a user's confidential property and cannot be recorded by anyone). Policies may be presented mathematically, as a list of allowed (secure) and disallowed (nonsecure) states. For our purposes, we will assume that any given policy provides an axiomatic description of secure states and nonsecure states. (BISHOP, c2005, p. 7).

Thus, it is possible to corroborate João (2012, p. 58) when he states that:

> [...] security has to do with preventing unauthorized access, alteration, theft, or physical damage to information systems. Controls, however, ensure the security of the organization's assets, the accuracy and reliability of its accounting records, and the operational adherence to administrative standards.

This goal can be achieved in the following ways: by separating the active threat of physical and / or logical; destroy the threat or move / destroy the asset. The destruction of the threat becomes impracticable, as it involves a complex process and may involve illegal actions. Destroy the active threat is quite undesirable from the point of view of the owner of the asset, and move it can be a very costly or even impossible process. So, there remains to be physically / logically separate from the threat's asset.

To accomplish this separation, it is necessary for the agency, institution or organization adopt a Security Policy Information and implements the mechanisms and procedures necessary for this policy to be enforced. As a definition of the Information Security Policy, stands out:

> Information security policy is a set of principles that guide the management of information security and that should be observed by the technical and managerial staff and internal and external users. The guidelines established in this policy determine the guidelines that must be followed by the organization to ensure its computational resources and information. (BRASIL. TRIBUNAL DE CONTAS DA UNIÃO, 2012, p. 10).

Bishop (c2005, p. 7) points out that it is important to explain the difference between Security Policy and security mechanisms:

> Definition 1–1. A security policy is a statement of what is, and what is not allowed. Definition 1–2. A security mechanism is a method, tool, or procedure for enforcing a security policy. Mechanisms can be nontechnical, such as requiring proof of identity before changing a password; in fact, policies often require some procedural mechanisms that technology cannot enforce.

Information security mechanisms include physical controls, which are considered as barriers that limit direct access to information or infrastructure, guaranteeing the existence of the information that supports it. To support these security mechanisms (physical controls: doors, shielding, guarding etc.), there are also logical controls, which are barriers that prevent or limit access to information that is usually in a controlled and electronic environment. One of the mechanisms that support logical control is cryptography. This, in turn, allows you to encode and transform the information in a way that makes it unintelligible to third parties, and to that end certain algorithms and secret keys are used to produce a sequence of data encrypted from the unencrypted data. As logical mechanisms, one can cite also: the digital signature; the functions of "Hashing" or checking; the mechanisms of access control (passwords, keywords, biometrics, firewalls, among others); And integrity and certification mechanisms and Honeypot, a program whose function is to detect and prevent the action of a cracker, hacker and spammer, or any other external agent. There are also a number of security tools and systems, such as antivirus, firewalls, AntiSpam filters, and more.

The Internet safety primer written by the Internet Steering Committee in Brazil (2012, p. 47-48) considers as basic safety requirements:

- **Identification:** to allow an entity to identify itself, that is, tell who it is;
- **Authentication:** Verify that the entity is actually who it claims to be;
- **Authorization:** to determine the actions that the entity can execute;
- **Integrity:** protect information against unauthorized alteration;
- **Confidentiality or secrecy:** protect information against unauthorized access;
- **No repudiation:** to avoid that an entity can deny that it was she who carried out an action;
- **Availability:** Ensure that a feature is available whenever needed.

Information security is not only Information Technology, as it involves legislation, technical standards, business and technology, and all these factors must be taken into account in the elaboration of an Information Security Policy. In view of this, Vieira (2014) prepared a compilation of the specific legislation related to information security (updated until August 14, 2014), which includes: Legal Devices of Federal Character; Specific Legislation of Federal Character; State / District Specific Legislation; Specific Legislation of Municipal Character; Technical Standards; Projects of Laws. (VIEIRA, 2014).

The management of information security and its implementation in organizations must also be carried out in accordance with the norms of the Brazilian Association of Technical Norms, specifically the "27000 family", and among others related. In addition, it is important to have a sense of the subject and related issues, such as: errors inherent in the use and manipulation of data (eg an email forwarded to the wrong recipient); Network attacks and data theft, counterfeits etc.; Actions of nature (earthquakes, storms, floods, among others) that could compromise physical structures, including those that safeguard backup data; Financial losses, legal proceedings, fines or contractual penalties; Damage to the image; And on key pests and cyber threats that leave IT resources vulnerable to attack, theft, and data manipulation.

2.2 Malwares

As previously shown, the information security is also a science. “Its theory is based on mathematical constructions, analyses, and proofs. Its system are built in accordance with the accepted practices of engineering. It uses inductive and deductive reasoning to examine the security of systems from key axioms and to discover underlying principles. These scientific principles can then be applied to untraditional situations and new theories, policies, and mechanisms”. (BISHOP, c2005, Preface, p. XXVII). Within this universe, one of the most common occurrences is the proliferation of malware that can inevitably compromise the security of the information and computers.

At the level of this study, viruses, malwares, and worms will be considered as the main plagues or virtual threats to which computers are constantly susceptible. According to João (2012), the generic term for malicious software programs is known as malware. Relating viruses and malwares, João (2012, p. 60) describes that:

> [...] They can be of various types including computer viruses, worms and Trojans. A computer virus is a program that attaches itself to others to run normally without the user noticing. Most computer viruses carry a load, which cannot cause major damage (just showing a message or image, for example), or be highly destructive, ruining programs, data and even reformatting the hard drive, among other things. [...]

Certainly, based on professional practice or the personal use of computers, there are many warnings about how dangerous it is to download files from unknown and / or dubious sources, and this is due to the fact that the viruses are commonly transmitted from one computer to another, either by sending an e-mail attachment or copy an infected file, or by other different actions.

Conceptualizing worms, João (2012, p. 62) states that:

> [...]They consist of independent computer programs, which are copied from one computer to the other through a network. The difference from viruses to worms is that they [...] can run on their own, without attaching themselves to other files, nor do they depend on human behavior to spread. [...]

For this reason, worms are spread much faster than viruses and act by destroying programs, files, data, etc., even interfering with the functioning of computer networks. It is usually stated that one of the characteristics that demonstrate that a computer has worms is exactly the slowness and the locking of the machine, since one of its actions is precisely to interrupt and to damage the operation of the computers.

In order to prevent these and other types of network-related problems, Herzog (2010) clarifies that security consists in separating the asset from the threats, in other words, "information security aims to ensure the integrity, confidentiality, authenticity and availability of the information processed by the organization". (BRASIL. TRIBUNAL DE CONTAS DA UNIÃO, 2012, p. 9).

In view of all this theoretical contribution, also documented in the form of decrees, laws and institutional documents, will be presented, next, the discussion about the performance of the librarian as one of the working professionals (working together with the IT professionals) in planning, in the elaboration and implementation of an Information Security Policy focused on the environments of academic libraries.

2.3 The Librarian's Action on Information Security

About the skills and professional performance of the librarian in the context of information security, Sobral (2012, online, emphasis added) clarifies that:

> According to the Brazilian Classification of Occupations - the Librarian belongs to the family of information professionals. Its main attributions are: to make the information available on any medium; Manage units such as libraries, information centers and correlates, as well as **networks** and **information systems**; Dealing technically and developing information resources; Disseminate information to facilitate access and knowledge generation; Develop studies and research; Carry out cultural diffusion and develop educational actions. **In order to carry out a task of such responsibility, it is necessary first of all to guarantee the security of the managed information, which is not only the usual concept of security, which is to ensure that something is not lost or that it falls into the wrong hands**. **Information security is also to ensure that information is available when needed and that its integrity can be guaranteed**.

In this sense, regardless of the nature and the public to which a particular library is intended, if its management is not sensitized to the issue of information security, the library will be subject to serious problems, such as misuse of target computers, including the risk of theft, leakage and loss of data. However, it is also necessary to take into consideration the conduct of users, since many of them do not take care when using public access computers, especially when they access e-mails and forget them open, or when accessing the online loan system to check your positions in the reserve queue, also forget to close the session, among many other examples that could be cited. After all, implicitly, users expect and trust that the library is responsible for keeping their data and equipment available in good condition, although they have not had any information or awareness of the cause, demonstrating that the librarian is facing another one Challenge: educate these users and prepare them for new practices and simple behaviors with respect to the security of their data and others. Faced with these threats and situations, it is noted how libraries must be prepared to deal with these problems.

It is worth introducing a relevant discussion, in which there will be deepening not being the main purpose of this article: What are the possibilities of using computers in a library? For research? For writing academic papers? To access various content on the Internet? To access social networks? All these questions, and many others that have not been asked, are important in order to know what dangers the library's network is exposed in order to be able to trace (in partnership with the institution's information and computer security team) what will be the best operational strategy for confronting of the risks to deal with these circumstances, without limiting the possibilities, freedoms and rights of users, and at the same time preserve and safeguard their data. In addition, a good plan of action is also needed to protect the network against attacks and vulnerabilities, and to safeguard and preserve the computers and equipment of the library, after all, as will be seen later, several computers in the libraries may be unprotected becoming target of attacks, espionage and pirated software installation that generate the proliferation of viruses and malwares, hijackers, unauthorized access to the entire

network, among other diseases. Regarding to information security, the managers of the institutions need to be aware that not only draw an outline of a policy, therefore it is necessary that this document contains consistent guidelines. This fact further reinforces the view that Academic Libraries have the need to establish their policy as soon as possible, since there are laws, decrees and federal determinations that validate the existence of an Information Security Policy in institutions. As an example, Decree 3505, dated June 13, 2000 (BRASIL, 2000), establishes the Information Security Policy in the organs and entities of the Federal Public Administration. Obviously, the implementation and application of an Information Security Policy should be established for the institution as a whole, regardless of whether it is in the public or private sphere, including libraries. However, this policy must be thought out, planned and elaborated in partnership with the sector responsible for Information Technology support, in addition to being well structured, to meet the objective it proposes. About the consistency of an Information Security Policy, it is agreed that:

> Security policies must have realistic implementation, and clearly define the areas of responsibility of users, systems management and personal networks and direction. It should also adapt to changes in the organization. Security policies provide a framework for the implementation of security mechanisms, define appropriate security procedures, security audit processes and establish a basis for legal proceedings in the attack sequence. (WEB ANEXO TECHNOLOGY, 2011, online).

Moreover, it defends the idea that just as the librarian should play its role in planning the preparation of this document is also necessary to have a division of responsibilities between the sectors of the institution, covering the library in the guidelines and actions established in common Agreement. In this sense:

> It is recommended that in the structure of the organization there is an area responsible for information security, which should initiate the information security policy making process, coordinate its implementation, approve and revise it, and designate security functions. It is worth notice, however, that people from critical areas of the organization should participate in the drafting process of the Information Security Policy, such as senior management and the various managers and owners of the computer systems. In addition, it is recommended that the Information Security Policy be approved by the highest leader of the organization. (BRASIL. TRIBUNAL DE CONTAS DA UNIÃO, 2012, p. 10).

In the scope of Academic Libraries, the planning of an Information Security Policy involves some access restrictions. This fact may generate some strangeness in the user, however, it is believed that the librarian can and should adopt an attitude that aims to sensitize the user about the importance of information security. Adopting this attitude, one must be prepared to face situations of dissatisfaction on the part of some of the users and with the clash of ideas that cause a healthy discussion between the class librarian and the users, with respect to the proposed measures in the Information Security Policy, besides having at hand another indicator to be evaluated in the libraries, in order to reach the speed, precision and security in the services offered through the use of the computers.

With regard to access restrictions, they should be included in the Information Security Policy and it should be noted that:

> **The fact that a user has been identified and authenticated does not mean that he can access any information or application without any restriction.** A specific control must be implemented, restricting the access of users only to the applications, files and utilities essential to carry out their functions in the organization. This control can be done by menus, functions or files. (BRASIL, 2007, p. 18, emphasis added).

As noted, to establish an Information Security Policy is also directly linked to actions that can be regarded as contradictory or controversial for users; however, all these bad impressions dissolved with the constant education of users, with the wide dissemination of Information Security Policy within the institution and the consolidation of an information security policy based on the principles of information security, and preferably managed By a larger instance than that of the Academic Libraries, always supported by the IT staff and the highest authority of the university. However, whatever the decision-making process, they must be documented and standardized so that everyone (without exception) complies with the guidelines set forth in the Information Security Policy. Based on this principle, Guelman (2006, p. 1) corroborates that "there is no point in investing in technology and physical protection if we do not have the collaboration and the commitment of the people".

The librarian must face yet another challenge related to the issue of information security, which is to provide and ensure access to the Internet, as the following excerpt, taken from the guidelines of the IFLA Internet Manifesto Guidelines (2006):

> Furthermore, the guidelines support the Declaration of Principles of the World Summit on the Information Society which was held in Geneva in 2003 and Tunis in 20052, and they also complement a declaration issued by IFLA during the World Summit on the Information Society process, the Alexandria Manifesto on Libraries, the Information Society in Action3. Both of these declarations stress a people-centred, inclusive and development-orientated society where all can access and share knowledge in an atmosphere of unrestricted access to information and freedom of expression. Against a background of these documents, the IFLA/UNESCO Internet Manifest guidelines document outlines service policies and procedures which safeguard freedom of access to information for all library users and ensure access to the Internet is free, equal and unhampered by unnecessary restrictions. (INTERNATIONAL FEDERATION OF LIBRARY ASSOCIATIONS AND INSTITUTIONS; UNITED NATION EDUCATIONAL, SCIENTIFIC AND CULTURAL ORGANIZATION, 2006, p. 10).

However, it is important to emphasize that the document itself has as its starting point the IFLA Internet Manifest Guidelines which has been providing wide and useful guidance since 2002, and in recent years, the Internet, users and information security landscape has changed considerably. Another important document is the Guidelines developed in 2006 and have since been translated into other languages and endorsed by IFLA, so some recommendations remain the same since that time. The IFLA Internet Manifest Guidelines alert to the fact that:

> **Technology changes; attitudes to what are the important issues change; and no set of guidelines can be regarded as providing answers for more than a short span of years**. If this document says less than might have been said on an issue that was at the top of everyone's mind five years ago, that is probably as it should be. If there is not such clear guidance as might be wished on an issue that may emerge as of central concern in twelve months time - the drafters do not claim clairvoyance. (INTERNATIONAL FEDERATION OF LIBRARY ASSOCIATIONS AND INSTITUTIONS; UNITED NATION EDUCATIONAL, SCIENTIFIC AND CULTURAL ORGANIZATION, 2006, p. 4, emphasis added).

The IFLA Internet Manifest Guidelines (2006, p. 15) also states: "While filtering is one of the issues most likely to cause contention in the library, there are also other downsides to the Internet that have to be considered". The guidelines further recognize that it is possible to create an Acceptable Use Policy (AUP), which:

> An **acceptable use policy (AUP) makes library Internet users aware of what is and of what is not acceptable use of library computers, and what sanctions there are if users breach the policy**. While AUPs will likely to differ from library to library, some parts of it are likely to be common to all – for example, those covering illegal use of the equipment (using a library's computers to access other computers without permission, for example). An AUP **should inform users of their responsibilities, which include both legal requirements and those defined by the library. The policy needs to provide the library with legal protection from liability, in that the AUP should make it clear to users that the library is not responsible for their actions on-line with regard to ecommerce and possible fraud by third parties resulting in losses to the user**. For example, an AUP would make it clear that all on-line transactions are at the user's risk, and are not the centre's responsibility. **The overall purpose of an AUP is to define a contract between the centre and the user - the policy should define the limits of the service, setting out what services are available and what would lead to those services being withdrawn**. (INTERNATIONAL FEDERATION OF LIBRARY ASSOCIATIONS AND INSTITUTIONS; UNITED NATION EDUCATIONAL, SCIENTIFIC AND CULTURAL ORGANIZATION, 2006, p. 29, emphasis added).

Therefore, Academic Libraries should prepare documents aimed at establishing general rules for the use of equipment and computational resources for the research, teaching, extension and administrative activities of Higher Education Institutions, so that threats are avoided or threatened. When creating institutional policies, such as guidelines, standards and rules, they should complement the Institution's Information Security Policy, not replace existing policies or even other documents that apply to the use of equipment and computing resources.

3 MATERIALS AND METHODS

The study makes use of action research as a guiding methodology for carrying out the work. According to Elliot (1997, p. 17), action research is a process that continually changes in spirals of reflection and action, where each spiral includes:

• Clarify and diagnose a practical situation or a practical problem that one wants to improve or solve;

• Formulate strategies for action;

• Develop these strategies and evaluate their effectiveness;
• Expand understanding of the new situation;
• Proceed to the same steps for the new practical situation.

The Figure 2 briefly explains this cycle:

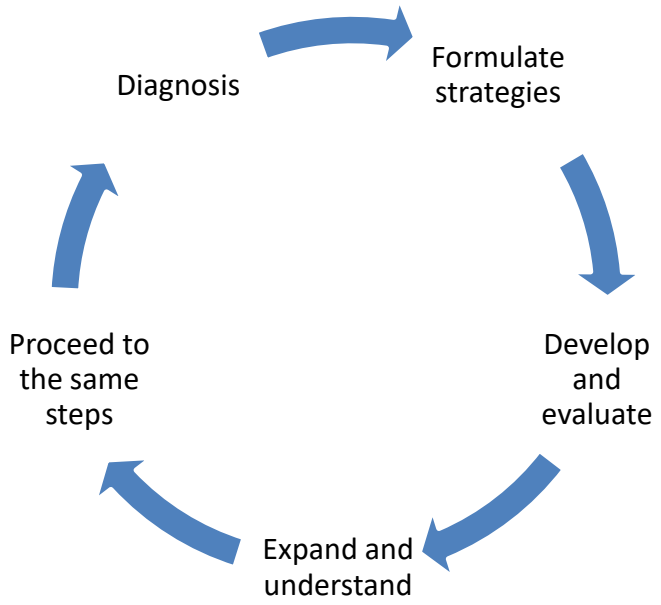

FIGURE 2. Spirals of action research.

Source: As prepared by the authors, based on Elliot (1997, p. 17).

Initially, a committee composed of six librarians met to outline the steps and actions to be followed for conducting site visits, held throughout the UFC Library System, 19 libraries in total. Thus, a partnership between the formed commission, the direction of the Library System and the Secretary of the University Information Technology, which resulted in the elaboration of a business schedule to the capital libraries and the interior was established (14 libraries).

In addition to the visits made in each library, observations and interventions made in the referral service of each unit were considered and recorded in form during the visitation, considering that it is the place where users are received, assisting them in their research, including it is the space where the perceived problems regarding the use of computers have been recorded. With regard to the form as a data collection instrument, designed to record the situation and diagnose the research computers in libraries, Vergara (2000, p. 55) considers it as "a compromise between interview and questionnaire". Appolinário (2004, p. 100) explains that the form is "Research instrument, similar to a questionnaire, but to be completed by the researcher himself (and not by the research subject) ". The pretest of the elaborated form was carried out in the libraries that attend to the areas of Human Sciences, Linguistics, Letters and Arts, incidentally, these were the units where the most serious cases were found.

Another characteristic of this research is its applied nature, descriptive and qualitative. According to Barros and Lehfeld (2000, p. 78), applied research has as motivation the need to produce knowledge for the application of its results, with the objective of "contributing to practical purposes, aiming at a more or less immediate solution of the problem in relation to reality". Complementing this statement, Appolinário (2004, p. 152) points out that applied research has the objective of "solving concrete or immediate problems or needs".

In addition to the methodological procedures, we used the literature, in order to compose the theoretical. Moreover, with the completion of the form, came to demand a document analysis and content after the visits because it was found that they are techniques that complement each other in relation to the proposed subject matter.

After the period of visits and based on the data obtained, the commission of librarians set as a goal the preparation of reports in order to document the reality found in libraries. From these reports, measures were suggested to be adopted in each unit, aiming to solve the problems encountered in order to guide future decision making.

In this sense, it was essential to use content analysis, which can be conceptualized as a set of intellectual operations that aims to describe and represent the content of the documents in a way different from the original, aiming to guarantee the retrieval of the information contained in it and make it possible its exchange, dissemination and use (IGLESIAS; GOMEZ, 2004). Therefore, such a technique is considered as the treatment of the content, in order to present it in a different way from the originating source examined, facilitating its consultation and referencing, that is, its purpose is to give convenient form and otherwise represent this information through in processes of transformation procedures. (BARDIN, 1997).

The analysis of the content of the reports was elaborated based on the data collection carried out during each visit to the libraries was then carried out. The contents of these reports present data referring to form fields, such as: computer asset number, machine operating system, used antivirus, installed text editors, videos and music player, browsing history, installed programs, responsible for computer maintenance in the information unit, maintenance request frequency, Wi-Fi Internet access and additional information.

Finally, it is pointed out that the guidelines for use and maintenance of computers for users of the Library System of the Federal University of Ceará, as well as guidelines for access to wireless Internet (Wi-Fi) in libraries, which were built as a result of the work, in view of the need for standardization in the configuration of the computers available to the academic community. Allied to this, it was necessary for the management to contribute to the dissemination of information security in the Library System, going directly to meet the proposal of the Information and Communication Security Policy prepared by the institution's own Information Technology Secretariat (UNIVERSIDADE FEDERAL DO CEARÁ, 2013).

All guidelines and documents were drawn up after the above steps and enabled the development of this study, the results of which will be presented below, more specifically the diagnosis and problems evidenced in the visits to the libraries and, based on the elaborated guidelines, the main topics that should fit the structure of a Security Policy Information.

4 RESULTS

The results of this research will be described based on the problems encountered during the visits in the libraries, whose report allowed the elaboration of guiding guidelines regarding the use and maintenance of the computers destined to the users as well as the suggestion of standardization of access to the Wi-Fi network inside the libraries. In addition, the description of the structure of an Information Security Policy will also be addressed as part of the results achieved.

4.1 Diagnosis and problems revealed from Visits to Libraries

The visited libraries are inserted in a diverse community of users, which vary according to the great areas of knowledge and with the undergraduate and postgraduate courses of the University. However, even within this diversity, some points in common have been identified. It has been seen that the problems evidenced will be presented on the basis of these common points, with the aim of avoiding unnecessary repetitions and protecting the names of the libraries in question.

First, the number of computers available to users in each library was counted, and whether these computers were intended solely for the collection of the collection or for other purposes, such as the production of academic papers and access to social media, for example. It was found that, in most libraries, there were specific computers for both cases: exclusive access to the online catalog, and other services of the Library System, and access to sites outside the University's domain. Even in the face of this reality, serious problems of infection in the machines were found, which made a detailed account of each situation necessary.

Another documented issue was about the maintenance of computers, more specifically who performs them (whether a library professional or STI), how often and based on what problems are detected. It was found that many of the libraries used one of the outsourced employees who were part of the team, in order to provide less complex support regarding the problems of the machines, although many of these employees do not have specific training in the area of informatics, acting, thus, in more routine situations. In more complex cases, requiring more advanced knowledge, most libraries were triggering the specialized services of the Department of Information Technology.

According to the reality found in libraries most computers used Windows 7 operating system, installed programs, text editors and video viewers, but some with audio disabled, even

though video viewers are enabled. In many computers, Windows updates were pending. One worrying aspect was the fact that many machines do not have any antivirus software installed or upgraded. This clearly demonstrates how computers were completely vulnerable to virus, malware, and hacker attacks. This situation also illustrates an over-reliance on the part of students, who believe they are protected when using the computers in the library or surf only safe areas, but actually are not always aware of the existing risks in using the Internet.

Another critical aspect was the fact that not all computers having dedicated software to access the sites allowed to control and run applications. This absence was reflected in a worrying access history. If, on the one hand, there were access to Web search engines, MSN Brasil, e-mails, Facebook, Digital Thesis and Dissertation Library, Institutional Repository, online catalog and other University's website domains; On the other hand there were also significant access to download sites of unknown and dubious programs, as well as visits to domains of infected sites already reported in leading Internet security and antivirus companies. Accessing non-recommended sites eventually made it possible for harmful tools that interfere with the settings to be installed on computers.

This scenario shows that the adoption of measures aimed at the security of computers was incipient until the moment of the visits, which resulted in a series of disorders and potentially dangerous situations regarding information security, such as:

Computers are viewed and the network is mapped by a certain user from one of the search engines, possibility of password theft or access to users' personal accounts, login and credit card data and online shopping saved in the computers and among other occurrences found.

Similar situations were observed in all the libraries. This frequency in the occurrence of certain problems indicates both aspects should be addressed as a priority in the implementation of an Information Security Policy, as well as the urgent need for librarians to devote more attention to such issues, either in the elaboration of institutional guidelines and policies, or in the Education and awareness of users.

Table 1 briefly presents the common problems highlighted in the visits to libraries:

TABLE 1. Results of the problems encountered in the visits to libraries.[i]

KNOWLEDGE AREAS	Exact Sciences and Earth and Biological Sciences (07 libraries); Social Sciences (04 libraries); Humanities and Linguistics, Arts and Literature (02 libraries); Health Sciences (01 library).
OPERATIONAL SYSTEM	Linux (Ubuntu e Kubuntu), Windows XP, Windows 7 e Windows 8.

ANTIVIRUS	05 libraries use; 08 libraries partially use (not installed on all machines or the license has expired); 01 library does not use.
PROBLEMS FOUND	Computers with obsolete settings; Pending operating system updates and various vulnerabilities; Infections found (viruses, cross-platform viruses [attacks all types of operating systems], malware, spyware, Trojan horses, backdoors, keyloggers, large number of hijackers, adware, spam, Potentially Unwanted Programs (PUP); Worms, files loaded with files saved by users, Wi-Fi Internet signal unrestricted, with unique password disclosure for any user and without proper control in most libraries; responsibility for maintaining the Wi-Fi network is shared with other sectors In some libraries in this category.
PRACTICES AND CONTROLS FOUND	Only 3 libraries of the 14 visited had access control and parental software on their computers; However, the tools proved to be ineffective in the face of the problems encountered; Only 02 libraries used access to the W-Fi network by access identified by the WUFCNet portal or application.
SITES ACCESSED (TYPES)	Banks (Internet Banking); Various blogs; Online catalog; University Library System; Emails; Various social networks; Academic information system of the University; News and gossip; Various newspapers; Collective Buying; Competitions; video classes; Video sharing sites with extensive search history and access to Mexican novels; File sharing sites; Various games; Telephone carrier sites (messaging service); Various databases; Digital libraries; lyrics; Download sites for series and movies; Various online shopping stores; Japanese comic book sites (manga); Extensive search history on sex news; Various slideshow sharing tools; Online dictionaries; Wikis.
INSTALLED SOFTWARE	Banks (Internet Banking); Text editors; Several extensions for browsers; Download managers; Various games; PDF readers; Audio and video players; 3D game plugins; Annotation synchronization program; Messaging / chat programs; Operating system optimizer programs; CD / DVD burning software; Video call softwares; Design software and calculations.
MAINTENANCE REQUEST	Yes (annually): 01 library; Yes (with no set frequency, it depends on the need): 13 libraries; No: 0 (zero) libraries.
WHO EXECUTES IT?	IT employee: 08 libraries; Outsourced employee: 05 libraries; Librarian: 04 libraries; Technical-administrative official without link with the Information Technology Secretariat: 03 libraries; Technical administrative staff of the library: 02 libraries. Note: In this option, some libraries fit into more than one condition; therefore, in some cases more than one item was marked on the form.

Source: As prepared by the authors.

According to the general picture presented in the table above, based on the analysis and diagnosis of computers, it is possible to perceive the need for alignment of actions and standardization of the service offered by libraries (research and open access computers). From the results found, a report was prepared for each library, containing the whole diagnosis, including suggestions for solutions to be applied, especially for libraries with the most serious

cases. These reports were sent to the Library System direction and then forwarded to each of the steering posts with their individual report per library.

Also during the visits, the question of access to the Wi-Fi network in each library was raised. Of the 14 libraries visited, 12 had open access in two distinct ways: without any restriction to internal and external users or through their own password, disseminating it on posters and at the service desk. In other situations, one of the libraries had a wireless network system, but the course secretariat was responsible for controlling the access and distribution of the password only for users connected to the course attended, that is, not even the library knew or had autonomy for this. In addition, another library only had Internet access via cable, as it did not yet have the necessary infrastructure to offer the wireless Internet service, and also experienced a situation similar to that of the library previously mentioned (the course secretariat provided Access passwords). Another case verified in the visits was the fact that one of the libraries did not have its own Wi-Fi signal, thus, it shared the access made available by the Academic Center of the course attended.

However, two libraries in the area of Exact Sciences offered the Wi-Fi access through the portal, and also application, called WUFCNet, developed by the Division of Computer Networks (DRC) of the Information Technology Secretariat, in which the user login is done with his CPF number and the password of the Integrated Academic Activities Management System (SIGAA). In addition to these two libraries, there were other sectors of the institution that had Wi-Fi access through this portal, although still in the testing phase. In view of this reality, the solution requested to Information Technology Secretariat was the suitability of all libraries for the proper use of the WUFCNet application, because it presents a more secure form of access in terms of user identification, being, therefore, chosen institutionally as the standard form to be included in the guidelines for accessing the Wi-Fi network in the libraries' dependencies, as will be seen later.

4.2 Structure of the Information Security Policy and Guidelines

Strategies and guidelines for the use and maintenance of computers and for the access to the Wi-Fi network in the libraries' dependencies were outlined based on the problems presented. (UNIVERSIDADE FEDERAL DO CEARÁ, 2015a; BIBLIOTECA UNIVERSITÁRIA, 2015b). In the scope of the document, the objectives, the procedures to be adopted in the libraries, the configuration of the research computers and of free access and the responsibility for the technical support to the machines were specified.

Thus, the procedures defined were:

a) Summon up the Information Technology Secretariat whenever there is a need for installation, maintenance and repair of the computers for research and free access of users, and

also extend to the working machines of the libraries, since there is a specialized team solely in meeting these demands in the University;
b) Request the adaptation of the operating system of the computers (Windows or Linux) to the library's need;
c) Request the reservation of a specific number of research computers exclusively to access the online catalog, to access the resources and services available on the library's website and in the University's domain;
d) Provide at least one computer with specific software and resources to enable access for persons with disabilities.

Regarding the configuration of computers used exclusively for research, the recommendations set forth in the guidelines were as follows:

a) Install the Linux operating system on the search engines, depending on the computer's factory configuration;
b) Maintain installed and updated operating system, antivirus and Internet browsers;
c) Create account and password of administrator and guest in each of the machines (the password of administrator being under the responsibility of librarians);
d) Block the installation of pirated and unauthorized software, and also the external pages to the domain of the University, with the exception of those characterized as being of academic research;
e) Install DosVox (program for the visually impaired), NVDA screen readers (for Windows) or Orca (for Linux), as well as other accessibility features in both operating systems;
f) Provide special stickers for keyboards in order to make them accessible to users with poor vision or other partial eye problems.

In order to compose the guidelines, free access computers were considered those whose access to domains outside the University (such as: e-mail accounts, social media, Web search engines, among others) or the library site is free. Therefore, it was emphasized, due to the requirement by the management of some of the libraries, the availability of computers for this purpose would not be mandatory and even those that have may suspend the provision of the service at any time. In this way, the configuration of these machines was conditioned to the following recommendations:

a) The number of computers reserved for users' free access, as well as their length of time on the computers, will be the responsibility of each library's management (there have been cases in which software tests have been carried out to regulate the time of permanence, or That even an employee has been designated for this purpose or if the operating system itself has been configured to deactivate the guest account after the time previously set by the library);
b) Depending on the computer's factory configuration, there may be machines with Linux or Windows operating system;
c) Maintain installed and updated operating system, antivirus and Internet browsers;

d) Access to sites that do not belong to the University domain is allowed, provided that the information security conditions adopted by the Library System and the institution are respected, in view of the guidelines presented in the Information and Communication Security Policy. (UNIVERSIDADE FEDERAL DO CEARÁ, 2013).

In regard to access to the Wi-Fi network in libraries, it should be noted that the University's Information Technology Secretariat had an already standardized portal and application, with login and password, in some sectors of the institution, and also in two of the 14 libraries visited. After applying the research and consequently analyzing the reports, it was found that this would be the safest way to standardize wireless Internet access, despite some resistance and contestation by users and librarians. The restriction of access to the Wi-Fi network was necessary in view of the signal quality itself, as well as the imminent threats to which it remains exposed. Thus, the following guidelines were established:

a) Access to the Wi-Fi network in the Library System is standardized through the portal and application developed by the institution's Information Technology Secretariat;
b) Users with institutional links have access to Wi-Fi through their Individual Registration Number (CPF) and their password of the Integrated System of Management of Academic Activities (SIGAA);
c) Users who do not have a link with the institution, that is, external public, visitors, distance education, extension projects of the University or outsourced employees, should resort to the temporary register as a guest in the portal or application of the Technology Secretariat of Information (the register of guests is conditioned to the completion of information about the user to be registered and can be done by any user with an institutional link, who will be responsible for the access of third parties that are linked to his Individual Registration Number);
d) The services offered by the portal developed by the Information Technology Secretariat, according to its use policy, are subordinated to the rules established by the respective providers and by the University.

With the objective of aligning these guidelines with the Information and Communication Security Policy (UNIVERSIDADE FEDERAL DO CEARÁ, 2013), the librarians' committee that was part of this work set as a goal the continuation of the composition of the Information Security Policy, a document structured by University since 2011, however, with considerable updates to be made. In partnership with the Department of Information Technology, the role of librarians is of fundamental importance to contemplate the University Libraries, in order to extend best practices documented in the guidelines and contribute to the IT industry, to strengthen some of the recommendations above listed formally on the Security Policy of the institution's information being discussed, improved and consolidated in its structure.

In this regard, the Information and Communication Security Policy is composed of: normative references; application field; introduction; scope; Concepts and definitions; principles; General guidelines, which include asset management, access control, auditing and

compliance, and continuity and risk management; Competences and responsibilities, assigned to the highest authority, the information and communication security management committee, the head of the Department of Information and Communication Security, as well as the department itself, and members of the institution, including University Libraries. In addition, the penalties, sanctions, update period and history of policy changes are also set out in the Information and Communication Security Policy, a guiding document developed in the Information Security Policy for the Library System.

Ideally, this Information Security Policy model, geared to the needs of University Libraries, should be prepared by a team of IT professionals in partnership with librarians and other professionals who can contribute to their vision of the sectors' operation, thus assisting in the construction of a well-designed Information Security Policy as based on their organizational needs, in addition to being defined by the highest level of the organization and approved by each direction.

The Information Security Policy, in its most general form, must take into account the requirements of the business strategy, regulations and legislation, as well as the environment of risks and threats to information security, making a diagnosis of the current situation and drawing up a prognosis. In addition, it should contain information security definitions, what are its objectives and the basic principles to guide all activities related to information security. The Information Security Policy should still contain the categorization of its public, the attribution of general and specific responsibilities, in order to address the management of information security, and the processes of handling deviations and exceptions, which should be foreseen in a contingency plan.

It is necessary that the preparation of the document be in an accessible, clear, simple and direct language, without going into technical details, so that all users and internal collaborators and external public can understand it. In addition, the Information Security Policy can be supported by specific policies of the subject (in this case, the University Libraries), detailed in such a way to consider the specific needs of the users as well as the interest of the organization. Some examples of this have already been mentioned in the guidelines presented above, but it should be pointed out that actions such as access control, physical security of the environment, backup and password policy, personal identification, among others, can and should be applied.

It is also important to highlight that the Information Security Policy should be widely disseminated and communicated to all users, directors, service providers, scholars, trainees, employees, employees, external audiences, among others, so that this information is Accessible and visible to all. In addition, it should be included in user education programs and corporate education, in order to raise awareness and draw attention to the importance of information security.

Regarding sanctions and penalties, these cannot be outside of an Information Security Policy, after all, the creation of guidelines, norms and rules requires this, since not always the people involved collaborate or follow them, and in these situations, Should be applied whenever pre-established policies are disregarded.

However, it is not enough just to elaborate and establish an Information Security Policy, since the document can and should undergo systematic and periodic revisions and modifications, or whenever necessary, aiming at the evaluation of opportunities, risk prevention, organizational changes in the work environment , Legal conditions, the emergence of new technologies, among other factors. All this in order to make a critical analysis and evaluate these policies and this should be left to the maximum manager and the management committee of the Information Security Policy. In short, it is necessary to know how to adapt the Information Security Policy to the reality of the institution, which guarantees the success of its implementation, especially when the librarian brings this responsibility.

5 CONSIDERATIONS

Knowing that it is the role of the librarian to manage the information resources available in the library, as well as to solve the problems of its information unit, this professional must be attentive to the new demands and prepared to handle the risk management in information security, going beyond the concern with maintaining computers. In fact, it is also the role of the library to monitor the proper functioning of its equipment and, if necessary, to pass on the demands to the relevant sector, but this alone does not constitute information security, although it is an integral part of a series of actions and best practices.

Concluding, in part, the discussion on this subject, it is known that the construction of an Information Security Policy is already a great challenge. Even more challenging is to develop a proper Information Security Policy for libraries, or even to include the universe of Academic Libraries in the institution's Information Security Policy. The managers of the Academic Libraries should keep in mind that these policies, as a rule, are consolidated in a general document, which is the Information Security Policy itself at the institutional level. Although often focused on the area of Information Technology, the ideal is that the Information Security Policy covers all aspects of information security in an organizational way, even for those who are not directly involved with computing resources.

In view of the above, in the current scenario that is configured, Academic Libraries should have as one of their priorities the implementation and inclusion of guidelines documented in an Information Security Policy, in order to comply with the International Information Security Standards, and that at the same time, contemplate the particularities and needs of an academic research environment, respecting, of course, the rights and freedom of users, as well as respecting the reality of each library, as well as meeting the Institutional Development of the Institution of Higher Education to which it belongs. Allied to this, it is of

paramount importance to standardize and to create norms of use of the computers for the research and the automated catalogs, without unnecessary extreme damages or restrictions that compromise the performance of the academic community to which the library attends.

Of course, the discussion about this theme can and should be more explored in the area of Librarianship and Information Science, mainly because some professionals already work with this or have affinity with the subject. In addition, there are those professionals who argue that there will not be any type of restriction applied to their users and their work team; therefore, there is a little or no information on security control. Still, it's hoped to have contributed greatly to the debate so that new ideas, discussions and solutions thrive in this field.

REFERENCES

APPOLINÁRIO, Fabio. **Dicionário de metodologia científica**: um guia para a produção do conhecimento científico. São Paulo: Atlas, 2004.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **Coleção ABNT**. Rio de Janeiro, 2014. Disponível em: <http://www.abntcolecao.com.br/ufc/grid.aspx> . Acesso em: 22 nov. 2014.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **NBR ISO/IEC 27001**: tecnologia da informação: técnicas de segurança: sistemas de gestão da segurança da informação: requisitos. Rio de Janeiro, 2013a.

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. Rio de Janeiro, 2013b.

BARCELO, Marta; HERZOG, P. **OSSTMM 3.0**: open-source security testing methodology manual. Nebraska: Institute for Security and Open Methodologies, 2010. Disponível em: <http://scadahacker.com/library/Documents/Assessment_Guidance/OSSTMM-3.0.pdf>. Acesso em: 10 fev. 2014.

BARDIN, Lawrence. **Análise de conteúdo**. Lisboa: Edições 70, 1997. 176 p.

BARROS, Aidil Jesus Paes de; LEHFELD, Neide Aparecida de S. **Fundamentos de metodologia**: um guia para a iniciação científica. 2. ed. São Paulo: Makron Books, 2000.

BISHOP, Matt. **Computer security**: art and science. Boston: Addison-Wesley, c2003. 968 p. Disponível em: <http://pt.scribd.com/doc/252378968/Computer-Security-Arts-and-Science-by-Matt-Bishop>. Acesso em: 24 dez. 2016. Erratas e materiais adicionais disponíveis em: <http://nob.cs.ucdavis.edu/book/book-aands/>.

BISHOP, Matt. **Introduction to computer security**. Boston: Addison-Wesley, c2005. 747 p. Disponível em: <http://www.uoitc.edu.iq/images/documents/informatics-

institute/exam_materials/Introduction%20to%20Computer%20Security%20pdf%20DONE.pdf>. Acesso em: 24 dez. 2016.

BRASIL. Decreto nº 3.505, de 13 de junho de 2000. Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal. Brasília, DF: Presidência da República. Casa Civil, 14 jun. 2000. p. 2. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto/D3505.htm>. Acesso em: 20 dez. 2016.

BRASIL. Decreto nº 5.903, de 20 de setembro de 2006. Regulamenta a Lei nº 10.962, de 11 de outubro de 2004, e a Lei nº 8.078, de 11 de setembro de 1990. **Diário Oficial [da] República Federativa do Brasil**, Brasília, DF, 21 set. 2006. p. 4.

BRASIL. Lei nº 12.527, de 18 de novembro de 2011. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. **Diário Oficial [da] República Federativa do Brasil**, Brasília, DF, 18 nov. 2011. Edição Extra, p. 1.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. **Diário Oficial [da] República Federativa do Brasil**, Brasília, DF, 24 abr. 2014. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 28 dez. 2016.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. **GSI realiza 5ª Reunião Ordinária do CGSI/2016**. Brasília, 2016. Disponível em: <http://dsic.planalto.gov.br/noticias/521-gsi-realiza-5-reuniao-ordinaria-do-cgsi-2016>. Acesso em: 22 dez. 2016.

BRASIL. Superior Tribunal de Justiça. Secretaria de Controle Interno. Coordenadoria de Auditoria de Tecnologia da Informação. **Cartilha de Segurança da Informação**. Brasília, [2014]. Disponível em: <http://www.stj.jus.br/portal_stj/arquivos/cartilha.pdf>. Acesso em: 10 fev. 2014.

BRASIL. Tribunal de Contas da União. **Boas práticas em segurança da informação**. 2. ed. Brasília, 2007. 70 p. Disponível em: <http://portal2.tcu.gov.br/portal/pls/portal/docs/2059162.PDF>. Acesso em: 10 fev. 2014.

BRASIL. Tribunal de Contas da União. **Cartilha de segurança da informação**. 4. ed. Brasília, 2012. 103 p. Disponível em: <http://portal2.tcu.gov.br/portal/pls/portal/docs/2511466.PDF>. Acesso em: 10 fev. 2014.

COMITÊ GESTOR DA INTERNET NO BRASIL (CGI.br). **Cartilha de segurança para internet**. 2. ed. São Paulo: CGI.br, 2012. Disponível em: <http://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf>. Acesso em: 29 dez. 2016.

COMITÊ GESTOR DA INTERNET NO BRASIL (CGI.br). **Neutralidade da rede no marco civil da Internet**. [2016]. Disponível em: <http://marcocivil.cgi.br/contribution/neutralidade-da-rede-no-marco-civil-da-internet/139>. Acesso em: 29 dez. 2016.

CONCERINO, Arthur José. Internet e segurança são compatíveis? In: LUCCA, Newton de; SIMÃO FILHO, Adalberto (Coord.). **Direito & internet***:* aspectos jurídicos relevantes. 2. ed. São Paulo: Quartier Latin, 2005. cap. 4.

ELLIOT, John. **La investigación-acción en educación**. Tradução de Pablo Manzano. 3. ed. Madrid: Morata, 1997. Disponível em: <http://goo.gl/vGU2wz>. Acesso em: 25 ago. 2016.

GONZAGA, Luiz. **Noções básicas de segurança da informação**. Fortaleza, 2014. 126 slides.

GUELMAN, Luiz. **Conscientização de usuários***:* como envolver seu público com a segurança da informação. In: MÓDULO SOLUTIONS FOR GRC. 08 ago. 2006. Disponível em: <http://www.modulo.com.br/comunidade/entrevistas/616-conscientizacao-de-usuarios-como-envolver-seu-publico-com-a-seguranca-da-informacao>. Acesso em: 15 dez. 2014.

IGLESIAS, María Elinor Dulzaides; GÓMEZ, Ana María Molina. Análisis documental y de información: dos componentes de un mismo proceso. **ACIMED**, Ciudad de La Habana, v. 12, n. 2, p. 1-5, mar./abr. 2004. Disponível em: <http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S1024-94352004000200011&lng=es&nrm=iso>. Acesso em: 26 ago. 2016.

INTERNATIONAL FEDERATION OF LIBRARY ASSOCIATIONS AND INSTITUTIONS (IFLA). UNITED NATION EDUCATION, SCIENTIFIC AND CULTURAL ORGANIZATION (UNESCO). **Diretrizes para o manifesto IFLA/UNESCO sobre a internet**. [Endossado pelo Conselho Diretor da IFLA em agosto de 2014 e atualizado (tradução em língua portuguesa) em novembro de 2014]. [Edinburgh], 2006. Disponível em: <http://www.ifla.org/files/assets/faife/publications/policy-documents/internet-manifesto-guidelines-pt.pdf>. Acesso em: 26 nov. 2014.

JOÃO, Belmiro. Segurança em sistemas de informação. In: _____. **Sistemas de informação**. São Paulo: Pearson, 2012. p. 58-70.

MANDARINO JÚNIOR, Raphael. **Segurança e defesa do espaço cibernético brasileiro**. Recife: Cubzac, 2010.

NAZARENO, Claudio. Entendendo as polêmicas e as mudanças trazidas pelo Marco Civil da Internet. In: CÂMARA DOS DEPUTADOS. Centro de Documentação e Informação. **Marco Civil da internet**. Brasília, DF: Edições Câmara, 2014. p. 9-27.

NUNAN, David. **Research methods in language learning**. Cambridge: Cambridge University Press, 1997.

OLIVEIRA, Maria Marly de. **Como fazer pesquisa qualitativa**. Petrópolis: Vozes, 2007.

SOBRAL, Fábio. Segurança da Informação: como garantir a confiabilidade e a integridade? **Biblioo**: cultura informacional, 5 mar. 2012. Disponível em: <http://biblioo.info/seguranca-da-informacao>. Acesso em: 10 fev. 2014.

REZENDE, Denis Alcides; ABREU, Aline França de. **Tecnologia da informação aplicada a sistemas de informação empresariais**: o papel estratégico da informação e dos sistemas de informação nas empresas. 3. ed. rev. e ampl. São Paulo: Atlas, 2003.

UNIVERSIDADE FEDERAL DO CEARÁ (UFC). **Plano de Desenvolvimento Institucional (PDI)**: 2013-2017. Fortaleza, 2012. p. 128, item 3. Disponível em: <http://www.ufc.br/images/_files/a_universidade/plano_desenvolvimento_institucional/pdi_ufc_2013-2017.pdf>. Acesso em: 22 abr. 2016.

UNIVERSIDADE FEDERAL DO CEARÁ (UFC). **Política de Segurança da Informação e Comunicação – POSIC**. Fortaleza, 2013. Disponível em: <http://www.sti.ufc.br/wp-content/uploads/2016/08/politica-seguranca-informacao-ufc.pdf>. Acesso em: 22 abr. 2016.

UNIVERSIDADE FEDERAL DO CEARÁ (UFC). Biblioteca Universitária (Comissão de Serviços). **Diretrizes para uso e manutenção dos computadores destinados aos usuários do Sistema de Bibliotecas da Universidade Federal do Ceará**. Fortaleza, 2015a. Disponível em: <http://www.biblioteca.ufc.br/images/arquivos/normativos/diretriz_uso_computadores_usuarios.pdf>. Acesso em: 20 abr. 2016.

UNIVERSIDADE FEDERAL DO CEARÁ(UFC). Biblioteca Universitária (Comissão de Serviços). **Diretrizes para o acesso à Internet sem fio (rede Wi-Fi) nas dependências do Sistema de Bibliotecas da Universidade Federal do Ceará**. Fortaleza, 2015b. Disponível em: <http://www.biblioteca.ufc.br/images/arquivos/normativos/diretriz_acesso_wifi.pdf>. Acesso em: 20 abr. 2016.

VERGARA, Sylvia Constant. **Projetos e relatórios de pesquisa em administração**. São Paulo: Atlas, 2000.

VIEIRA, Tatiana Malta. **Compilação de Legislação específica relacionada à segurança da informação (atualizada até 14 de agosto de 2014)**. Revisor Josemar Andrade Fraga. Brasília, DF: Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República (DSIC/GSI/PR), 2014. Disponível em: <http://dsic.planalto.gov.br/documentos/quadro_legislacao.htm>. Acesso em: 20 dez. 2016.

WEB ANEXO TECHNOLOGY. **Segurança da informação**. Criado em 20 jul. 2011. Disponível em: <http://www.anexotechnology.com.br/projetos_seginfo.html>. Acesso em: 10 dez. 2014.

ACKNOWLEDGEMENTS

The authors thank the librarians: Ana Elizabeth Albuquerque Maia; Ericson Bezerra Viana; José Jairo Viana de Sousa; Kalline Yasmin Soares Feitosa; Mara Roxanne de Souza Santos and Vanessa Pimenta Rodrigues Simões. They are also grateful to the Professors Edson Alencar and Elzenir Coelho for the review and translation of this article. They are also grateful to the directors of the UFC's 14 libraries, who kindly contributed to the responses to the research form.

[i] As the overall picture presented concisely in Table 1, the areas of knowledge covered by the Federal University of Ceará's Library System were included. The division by area was the closest possible to the courses present in the campuses that the libraries attend; Thus, there may be more than one area of knowledge specified for each library group. For further details of the conditions found in each library, there is a more complete picture which can be found in additional documents this article.